NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

WEB-BASED NETWORK MANAGEMENT TOOLS FOR U.S. NAVY MISSION-CENTRIC APPLICATIONS

by

Eric L. Andalis

September, 1997

Thesis Advisor:	Rex A. Buddenberg
Second Reader:	Suresh Sridhar

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1997	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE : WEB-BASE NETWORK MANAGEMENT TOOLS FOR U.S. NAVY MISSION-CENTRIC APPLICATIONS	5. FUNDING NUMBERS
6. AUTHOR(S) Andalis, Eric L.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited.	

13. ABSTRACT *(maximum 200 words)*

The purpose of this thesis is to propose a Web-based interface solution to the Navy's mission-centric network management needs. A Web-based interface provides an easy to manipulate, universal client that can be accessed from any desktop that is connected to the Internet. A Web-based interface can be designed to show decision-makers and managers the status of network-centric information and how it affects the mission of Navy units.

This thesis also briefly describes basic network management techniques and the use of the Navy's Automated Digital Networking System (ADNS). As the Navy adopts a network-centric approach for every day business, including warfighting, network management becomes extremely critical. Commercial products can't fulfill all Navy specific requirements. The use of the Web is a solution to provide mission-centric network management information to the manager and decision-maker in an easy-to-use environment.

14. SUBJECT TERMS Network Management, Web-based Network Management, Automated Digital Network System, ADNS	15. NUMBER OF PAGES 129
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std.

239-18

Approved for public release; distribution is unlimited

WEB-BASED NETWORK MANAGEMENT TOOLS FOR U.S. NAVY MISSION-CENTRIC APPLICATIONS

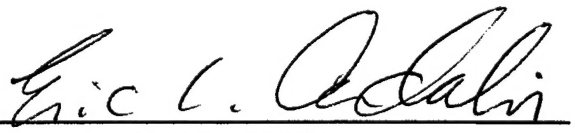
Eric L. Andalis
Lieutenant, United States Navy
B.A., University of California, San Diego, 1989

Submitted in partial fulfillment of the
requirements for the degree of

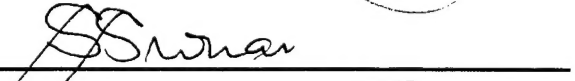
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

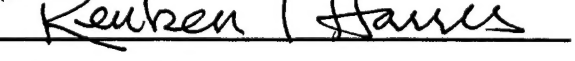
from the

NAVAL POSTGRADUATE SCHOOL
September, 1997

Author: 
Eric L. Andalis

Approved by: 
Rex Buddenberg, Thesis Advisor


Suresh Sridhar, Second Reader


Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

The purpose of this thesis is to propose a Web-based interface solution to the Navy's mission-centric network management needs. A Web-based interface provides an easy to manipulate, universal client that can be accessed from any desktop that is connected to the Internet. A Web-based interface can be designed to show decision-makers and managers the status of network-centric information and how it affects the mission of Navy units.

This thesis also briefly describes basic network management techniques and the use of the Navy's Automated Digital Networking System (ADNS). As the Navy adopts a network-centric approach for every day business, including warfighting, network management becomes extremely critical. Commercial products can't fulfill all Navy specific requirements. The use of the Web is a solution to provide mission-centric network management information to the manager and decision-maker in an easy-to-use environment.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND/OR ABBREVIATIONS

AAW	Anti-Air Warfare
ACSE	Association Control Service Element
ADNS	Automated Digital Networking System
ARPANET	Department of Defense's Advanced Research Projects Agency
ASCC	Autonomous System Control Center
ASN	Abstract Syntax Notation
ASUW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
CIO	Chief Information Officer
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
COMMPLAN	Communications Plan
DOS	Department of Defense
GUI	Graphic User Interface
HMMP	HyperMedia Management Protocol
HMMS	HyperMedia Management Schema
HMOM	HyperMedia Object Manager
HP-NNM	Hewlett-Packard Open View Network Node Manager
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ICMP	Internet control Message Protocol
IETF	Internet Engineering Task Force
JMAPI	JAVA Management Application Programming Interface
LAN	Local Area Network
LCC	Local Control Center
MAN	Metropolitan Area Network
MIB	Management Information Base
NIPRNET	Unclassified but Sensitive IP Router Network
NOC	Naval Operations Center
NRaD	Naval Command, Control and Ocean Surveillance Center
NMS	Network Management System
NPS	Naval Postgraduate School
OSI	International Organization for Standardization
PDU	Protocol Data Unit
PING	Packet Internet Groper
RFC	Request For Comment
RMON	Remote Nework Monitoring
ROSE	Remote Operations Serve Element
SIPRNET	Secret IP Router Network
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	Wide Area Network
WBEM	Web-based Enterprise Management Architecture
WWW	World Wide Web

ACKNOWLEDGEMENT

The author would like to thank Professors Buddenberg and Sridhar for their time and patience. The author would like to specially thank Bill Jacobs of NRaD RDTE Div, for his time and tutelage of the subject matter in this thesis. The author would also like to acknowledge the following contributing personnel:

- Lou Gutman of NRaD, RDTE Div
- Roger Casey of NRaD, RDTE Div
- Chris Barber of Mitre Corp.
- LCDR Jim Sullivan
- LT Brian Rehard

Most of all the author would like to thank his wife, Katherine Andalis, for all of her enduring support and patience during the often stressful times spent on school assignments and this thesis.

I. INTRODUCTION

The Navy is currently adopting a network-centric approach to accomplish its tasks and missions. Because of technological breakthroughs in wireless data communications, the Navy is now able to bring desktop real time data transfer capabilities to underway units with developments in the Automated Digital Networking System (ADNS). This brings about a maturity and shift from traditional methods of technical control troubleshooting in the radio room to a network-centric approach for managing future Navy networks. Network management is critical to any organization but even more so to the military. The military will be increasingly reliant on networks as it supports combat effectiveness and readiness, which ultimately makes networks crucial in the role of national and international security.

However, network management is a complex task that requires expert knowledge in many areas. To successfully manage networks, the right people and the right tools are required. ADNS brings the necessary tools for data transfer capability such as hardware and software. However, there is still much development in the area of methods and principles to be used to manage the Navy's networks. There are commercial Network Management Systems (NMS) available to manage universal objects such as Routers, Hosts, and Connectors. However, there are still many issues on how to manage the network as it supports unique military operations and missions.

There are other issues of how the network will impact traditional military customs and cultures. Although the goal is to increase efficiency and savings, networks bring about many challenges to the hierarchical structure of the chain of command. This is an exciting time to be in the military as members get to participate in a revolution or

evolution of military affairs. Time will only tell where the successes and failures will take place.

This thesis describes the basics of network management and offers a prototype solution for unique Navy requirements for network management. Chapter II describes the problem of unique network mission requirements for the Navy. Chapter III gives a quick overview in fundamentals of network management, including requirements and protocols. Chapter IV is a broad description of ADNS. (a revised Chapter IV has also been submitted by this thesis author and two other NPS students (LCDR Jim Sullivan and LT Brian Rehard) as a separate Informational Request For Comment (RFC) to the Internet Engineering Task Force (IETF) to make ADNS public). Chapter V describes the prototype developed for a Web-based network management tool for the Navy. Appendix A identifies some unresolved network management issues.

II. PROBLEM STATEMENT

The Navy's unique roles and missions often require tailored applications to carry out these responsibilities. Although there has been a recent shift towards buying commercial products to save money, there are particular needs that require specialized development to provide the necessary tools to ultimately support the warrior.

As the Navy becomes 1) network-centric and 2) adopts mainstream Internet technology to extent feasible, a major emphasis will be to manage these networks. However, managers and high level decision-makers may not want to know the specifics about network management but will probably want to know how the network affects certain unit levels and the missions assigned to those units. An easy user interface is also desired to present this information. Viewing different military networks and systems as nodes attached to an Internet allows: 1) a robust infrastructure which includes and leverages commercial technology and 2) permits inclusion of military specific technology and implementations where required.

Using the World Wide Web (WWW) is an excellent tool for these kinds of applications goals. Web pages are easy to read and easy to manipulate. Web pages are also accessible from any connection to the Internet (a universal client), which makes it accessible from any desktop, anywhere. The Web sites would have to be individually tailored to different command and control levels and would have to be updated on a constant basis. Using the Web allows anybody from high-level decision-makers to unit level managers to view the same information about how the network affects the mission of particular unit levels.

III. NETWORK MANAGEMENT

A. NETWORK MANAGEMENT OVERVIEW

Chapter III reiterates basic network management concepts. To understand the impact of network management on Navy networks, it is notable to highlight some of the network management standards and technologies that exist and are up and coming. The eventual goal is to increase combat effectiveness with less manpower through the use of remote network management. For example, in future ship designs, the ability to isolate certain compartments and fight a shipboard fire can be possible through the use of SNMP agents shutting shipboard hatches and activating firefighting chemicals. Shipboard architectures can be monitored and managed remotely through on one management station. Therefore it is significant to go over some basic network management techniques. However, if the reader is already knowledgeable in these areas, I recommend skipping this chapter.

Networks today have exploded into complex and tangled systems. As organizations adopted Local Area Networks (LANs), Wide Area Networks (WANs), and Metropolitan Area Networks (MANs), the next logical step was to adopt clear techniques and tools to properly tame these beasts. Organizations have become totally reliant on their networks and could experience devastating results if inefficiency or down time was encountered. The network managers' and administrators' jobs became increasingly critical to the health of organizations and proper knowledge and tools are part of an efficiently running network. Although many steps have been taken and devised to successfully manage networks, much progress is still being made in network management. Network management can be defined as the processes and techniques to

ensure an organization's network is operating properly and efficiently (Leinwand and Conroy, 1996).

Network management consists of numerous elements of the network. However, these elements can be simplified into certain categories: agents, protocols, management information bases, and a management center running a network management platform. Agents are objects such as hardware components or software applications that contain special software that allow that object to be monitored and managed. Protocols allow agents to communicate with the network management platform. Management information bases contain information about agents that allow network managers to monitor objects. A network management platform is a software program that allows managers to monitor and supervise objects that carry agents. Each one of these entities make up the Network Management System (NMS) (Leinwand and Conroy, 1996).

B. NETWORK MANAGEMENT AREAS

Network management can be divided into specific functional areas that were divided by the International Organization for Standardization (OSI) into: fault management, accounting management, configuration management, performance management, and security management. Fault management includes the methods and procedures for managers to locate, isolate, and correct any faults experienced in the system. This includes ways in which the network management platform is automatically notified of any faults in the system. As time becomes a critical factor in an organization's operation, fault management's importance is apparent. Accounting management is associated with the costs of the use of the network. It includes properly tracking and charging of different subsets of the organization for the use of the network. This becomes

important since managers need to allocate resources accordingly. Configuration management involves managers manipulating different hardware and software aspects of the system while keeping the whole system operating. This is done due to many reasons such as shutting down faulty nodes for troubleshooting or upgrading the system. Proper care and notification must be taken since many nodes are inter-related with each other. Performance management tries to ensure that resources are within certain thresholds. Managers have to monitor and control such occurrences as excessive data traffic and proper response time. Security management requires managers to properly protect the system from such dangers as: human error, abuse of authority, direct probing, penetration, and subversion. This includes such procedures as adopting proper encryption techniques and security logs (Stallings 1993).

OSI Functional Areas of Network Management	Description
Fault Management	The function of detecting, isolating, and correcting faults in the system.
Accounting Management	The function of properly tracking and charging the system's resources to users.
Configuration Management	The function of manipulating hardware and software while still maintaining the system.
Performance Management	The function of properly monitoring and controlling the system's resources.
Security Management	The function of protecting the system from such dangers as human error, abuse of authority, direct probing, penetration, and subversion.

Table I. OSI functional Areas of Network Management

C. NETWORK MANAGEMENT PROTOCOLS

What allows the network manager to communicate with the network to accomplish the above goals? The adoption of standard protocols allows managers to monitor and control data efficiently run the network. The most common network management protocol found in objects is the Simple Network Management Protocol (SNMP), its popularity grew alongside the Transmission Control Protocol/Internet

Protocol (TCP/IP) for good reasons. In the late 1970's, TCP/IP grew from the Department of Defense's (DOD) Advanced Research Projects Agency (ARPANET) to transfer data among different terminals while still keeping interoperability. TCP/IP proved to be such a robust and mature protocol that non-military applications soon began to adopt it, thus exploded the exponential growth rate of the Internet.

With the exponential growth of nodes on the Internet, there soon became an apparent need for network management standards. The Internet Control Message Protocol (ICMP) was used as an early means to gather simple information about nodes utilizing IP. ICMP was commonly used with a capability to echo and echo-reply communications with objects such as hosts and routers. A program called Packet Internet Groper (PING) then became widely used with ICMP to communicate with objects. PING basically determined network connectivity between objects. A manager would instigate a PING echo from a source host. The destination device would then respond with an echo reply giving such information as: response time, number of data packets sent, data packets received, and data packets lost. However, much of it's disadvantages stem from limited information provided and the need for polling. A manager would need to continue polling devices to obtain up-to-date information. There became an obvious and quick need for better solutions as the Internet quickly grew (Leinwand and Conroy, 1996). Although different protocols are explained below, SNMP remains the most common today. Only a few common protocols will be explained to just give a flavor of some of the requirements for network management. There are many arguments about the future of protocols such as the choice between SNMP and CMIP.

However, as the Internet continues to grow exponentially, users will eventually and continually decide the fates of these protocols.

1. SNMP

SNMP was a quick answer to provide managers with tools for network management. Although there exists many other protocols for network management, SNMP like TCP/IP may have some limitations, but will still be around for many years due to it's popularity. SNMP's basic functions can be summarized into the following three operations: *get, set,* and *trap.* These operations utilize a central collection of data in each object called the Management Information Base (MIB). It is important to first explain the MIB prior to describing the basic functions of SNMP. See *RFC 1157* for specific SNMP information.

a. Management Information Base (MIB)

The MIB is simply a two dimensional database in which data about certain objects is collected. The MIB can then be accessed by a management platform to gain and manipulate information about those particular objects. The MIB can only store scalars and two-dimensional arrays of scalars, which holds some limitations. However, the beauty of this structure is its simplicity. See *RFC 1155* for specific MIB information. This structure is in a form of a hierarchical tree in accordance to Abstract Syntax Notation One (ASN.1) standards. The key data types in a MIB are (Stallings, 1993):

- *SYNTAX*: the general structure of the data type. It allows for definition and specification.
- *ACCESS*: the way an object will be accessed like through SNMP. Values can be "read-only," "read-write," "write-only", and "not-accessible"

- *STATUS*: shows the implementation support required for the object. Values can be "mandatory", "optional", "deprecated", or "obsolete".
- *DescrPart*: an optional field describing the object type.
- *ReferPart*: another optional field, cross-referencing the object to other MIB information.
- *IndexPart*: used to define tables.
- *DefValPart*: an optional field to define acceptable default values.
- *VALUE NOTATIONS*: name used to access the object via SNMP.

Tables also have a standard format in a MIB. They are two-dimensional with scalar values (Stallings, 1993):

- *State*: the state of one of eleven TCP connections such as: closed, listen, established, etc.
- *Local address*: the IP address of this end of connection.
- *Local port*: the TCP port of this end of connection.
- *Remote address*: the IP address of the other end of connection.
- *Remote port*: the TCP port of the other end of connection.

b. *Get, Set,* and *Trap*

The operations of SNMP can be broken down to three basic commands: *get, set,* and *trap.* These commands utilize the MIB to obtain and manipulate data pertaining to objects. *Get* allows a manager to obtain data from and object. *Set* allows a manager to change or update data from an object. *Trap* sends data automatically from an object to a manager when certain thresholds are exceeded.

Through the use of MIBs, SNMP agents can be installed on and allow managers to monitor specific objects. This is very useful to the Navy, since SNMP allows engineers to design MIBs for such legacy hardware as radars and tranceivers. A good example is the one given in the beginning of this chapter pertaining to the ability to isolate a shipboard fire through the use of SNMP agents.

When a management platform would like to query an agent, it sends a Get-Request message and the agent first checks the packets for such things as compatibility and authentication and sends back a Get-Response message. The Get-Request message includes the following fields in the Protocol Data Unit (PDU) (Stallings, 1993):

- *PDU type*: a Get-Request PDU.
- *request-id*: a unique identifier for receiving agents to correlate incoming responses and outstanding requests.
- *variable-bindings*: list of objects and data requested.

The Get-Response message simply returns the values in the variable-bindings to the management platform. Such information can include: duration of objects running and how many nodes are up in the system. A Get-Next-Request message is often used with a Get-Response message to obtain the next object in a table until no more values are found.

A Set-Request message can be used by a manager to change data values. This is often done to change certain thresholds in objects so that a *trap* message can or not be sent. It also allows for some simple configuration techniques such as shutting down or rebooting a host if the Get-Response message holds a certain value.

A *trap* message is automatically sent to a management platform by an object if certain thresholds are exceeded. Such threshold examples include: disk space

limitations, physical connections changed, or a node being down. The following fields identify the *trap* PDU (Stallings, 1993):

- *PDU type*: *trap* PDU id.
- *enterprise*: which sub-system instigated the *trap*.
- *agent-addr*: IP address of *trap* object.
- *generic-trap*: a predefined *trap* type.
- *specific-trap*: a specifically defined *trap*.
- *time-stamp*: time between last re-initialization and generation of *trap*.
- *variable-bindings*: additional specific information.

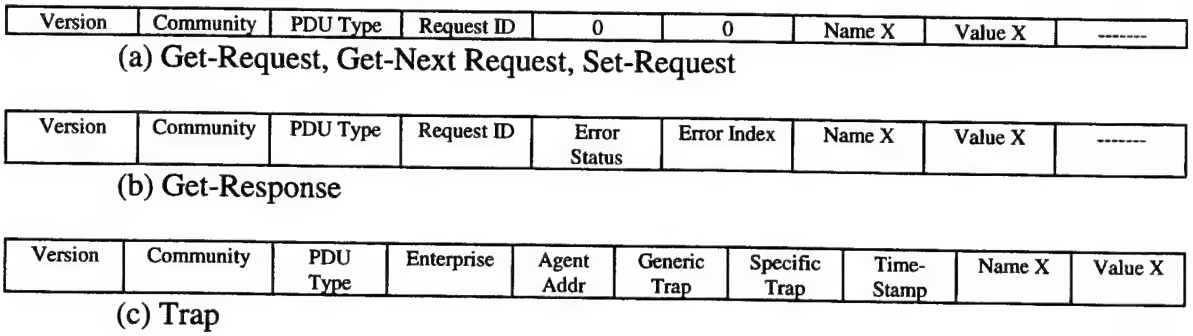


Figure 1. SNMP Message Composition. After Ref [Leinwand & Conroy].

The simple SNMP commands, a manager can communicate with any object with an agent. This was especially useful remotely (through the Internet). However this had the potential for abuse. Authenticity was a problem when commands were sent remotely. However, security features were deliberately omitted from SNMPv1 due to the problems of standardization of the public key cryptography systems. Some of these security solutions were solved by vendors, proprietarily. However, in the early 1990's a solution to the security problem was offered and became what is known as SNMPv2.

2. SNMPv2

The increased security enhancements of SNMPv2 deal with: privacy, authentication, and access control. Privacy allows for only the intended receiver to obtain the message. Authentication is to ensure that the sender is really who they say they are. Access control allows for only authorized users to certain data.

Currently, SNMPv2 seems to have lost some forward movement and is not widely adopted. However, because of the sensitivity of Navy operations, it is entirely possible for the Navy to adopt pre-standard SNMPv2 for it's security functions.

a. SNMP v2 Message Format

The message formats are similar between SNMP and SNMPv2. The Get-Request, Get-Next-Request, Get-Response, Set-Request, and Trap messages as in Figure 1 are converged into one message format for SNMPv2 except for Get-Response. Two message formats are added: InformRequest and GetBulkRequest which address scalability issues. InformRequest allows for manager to manager communications. The GetBulkRequest allows for the collection of large amounts of data without retrieving each data field one at a time as the Get-Next-Request message does (Leinwand and Conroy, 1996).

PDU Type	Request ID	0	0	Name X	Value X	----------

(a) Get-Request, Get-Next-Request, Set-Request, Trap, InformRequest

PDU Type	Request ID	Error Status	Error Index	Name X	Value X	----------

(b) Get-Response

PDU Type	Request ID	Non-Repeaters	Max Repetitions	Name X	Value X	--------

(c) GetBulkRequest

Figure 2. SNMPv2 Message Composition. After Ref [Leinwand & Conroy].

b. Privacy

Three variables describe the protocol pertaining to privacy (Stallings, 1994):

- *partyPrivProtocl*: the means by which messages are received are protected.
- *partyPrivPriv*: secret value to unlock the privacy protocol.
- *partyPrivPublic*: public value to unlock the privacy protocol such as a public encryption key.

The term *party* refers to the whole scheme in which SNMPv2 entities exchanges messages.

c. Authentication

Five data fields allow the protocol for authentication (Stallings, 1994):

- *partyAuthProtocol*: means by which messages are authenticated.
- *partyAuthClock*: current time.
- *partyAuthPrivate*: secret value to unlock the authentication protocol.
- *partyAuthPublic*: public value to unlock the authentication protocol such as a public encryption key.
- *partyAuthLifetime*: a lifetime limit for messages.

d. Access Control

SNMPv2 utilizes MIB views called contexts for access control. A context is simply the collection of managed objects, locally or remotely, that a manager has access to. When a subject (SNMP party requesting information) requests information from a target (SNMP party being requested), a privileges database is checked for allowable access to a certain context (Stallings, 1993).

3. Remote Network Monitoring (RMON)

The goal of remote network monitoring is to analyze data across whole portions of the network such as a LAN through the use of monitors, sometimes called analyzers or probes. These monitors can analyze data packets defined in the RMON MIB across a LAN in what is called *promiscuous mode*, that is passively listening to all data packets on that certain segment. *RFC 1271* and *1757* give more details about RMON.

a. RMON Goals

RMON goals can be defined in five different areas (Leinwand and Conroy, 1996):

- *off-line operation*: it is too costly for a network management platform to continually poll devices. The RMON device allows for the accumulation of data and would contact the management platform in case of an anomaly.
- *preemptive monitoring*: the RMON device continually runs diagnostics and monitors network performance. In case of a failure to the segment, the RMON device gives the manager helpful diagnostic information.
- *problem detection and reporting*: the RMON device can detect errors without polling devices. A device can be configured to notify the management station and log the abnormal conditions being experienced. This frees the management station to having to conduct the same operation, thus freeing up traffic and resources.
- *value-added data*: the RMON device can be dedicated to analyze information about that particular segment. Again, this saves resources by freeing up the

management station from this requirement. Such things can be analyzed such as finding the most problematic hosts in terms of errors and traffic.

- *multiple managers*: more than one network management station is often used for reliability and separate duties. The RMON device allows it to communicate to multiple managers separately.

b. RMON MIB

The RMON MIB is divided into nine different functions and groups (Leinwand and Conroy, 1996):

- *statistics group*: provides some statistics for each interface on the RMON device. These statistics are separated for each interface, allowing for better management.
- *history group*: allows for storing periodical data for later analysis.
- *alarm group*: allows for certain thresholds to be set over a period of time. If these thresholds are exceeded, an alarm would be sent to the manager.
- *host group*: allows for management of traffic associated with each host on the segment.
- *hostTopN group*: prepares statistic reports on hosts specified in the management platform. The "N" stands for the number of hosts with the statistics specified. For example, the top ten hosts in terms of message traffic.
- *matrix group*: keeps in matrix format, the number of packets, bytes, and errors between two nodes. This allows for performance management of two nodes.
- *filter group*: allows for the analysis of specific data. When a packet matches the filter, it is sent up a separate channel.

- *packet capture group*: buffering scheme to capture packets from the channels in the filter group.
- *event group*: logs events into a table when specified events occur which allows for an audit trail.

RMON can be an important tool for the Navy. It provides two important functions. One, it will improve the integrity of the communications system, which ultimately improves combat effectiveness. Two, it offsets the need for personnel to manage the network both on ships and ashore. It provides a means for managers to monitor and manage networks remotely from ships or shore.

4. Common Management Information Service (CMIS)

The Common Management Information Protocol (CMIP) was developed to overcome many of the limitations of SNMP. The main differences are that CMIP relies on managed objects to share more responsibility in the NMS, where SNMP relies heavily on the management station. CMIP allows a complete protocol suite for any object. It does this over the OSI seven layer reference model in conjunction with the Common Management Information Service (CMIS). To better understand CMIP, a brief explanation of CMIS is required.

CMIS defines the communication requirements for the OSI model. In the application layer (7) of the OSI model, any network application that deals with CMIP is considered a Common Management Information Service Element (CMISE). CMISE also uses two other applications called Association Control Service Element (ACSE) and Remote Operations Serve Element (ROSE) to handle interactions between applications.

There are three different services for CMIS: association, management-notification, and management-operation (Leinwand and Conroy, 1996).

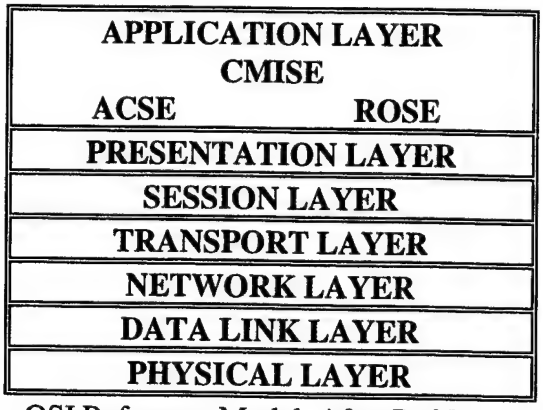


Figure 3. CMIP in OSI Reference Model. After Ref [Leinwand & Conroy].

a. Association Service

Management association controls the associations between applications. Three commands describe the management association service:

- M-INITIALIZE: opens the association between applications.
- M-TERMINATE: closes associations.
- M-ABORT: closes associations during abnormal operations.

b. Management-Notification Service

This service gives information to a notification similar to an SNMP *trap* message. The M-EVENT-REPORT command gives the management information.

c. Management-Operation Service

The operation service utilizes six commands to receive management information, similar to the SNMP *get* message.

- M-GET: used to retrieve information.
- M-CANCEL-GET: used to cancel a previous request.
- M-SET: used to modify information.

- M-ACTION: used to perform an action.
- M-CREATE: used to create an instance of a managed object.
- M-DELETE: used to delete an instance of a managed object.

5. Common Management Information Protocol (CMIP)

CMIP implements CMIS by defining the rules of association between applications using a CMIP machine. The commands above show the efficiency and versatility of CMIP over SNMP. It allows functions not possible with SNMP. However, there are many shortcomings that have limited CMIP from being the protocol of choice. It's largest disadvantage is the amount of overhead required. Because of this, many organizations have avoided CMIP due to cost of the systems able to handle CMIP. The other primary disadvantage is the difficulty of implementation. It's difficult to program due to the number of variables required (Concentric).

D. WEB-BASED NETWORK MANAGEMENT

A relatively new tool for network management is using the World Wide Web (WWW). The answer is quite obvious due to the Web's commonality and ease of use (standard client). Web-based tools allow users to interface information with simplicity and mobility. Increasing capabilities of Web products allow information to have such popular features as graphics and multimedia. A Web-based network management allows managers to have access to information from any desktop due to the popularity of Hyper Text Transfer Protocol (HTTP) in a client-server environment which provides a means to have access to information in a non-proprietary manner. This also allows the ability to manage network information from virtually any location on any machine. Although there are disadvantages of using the Web such as overhead and resource requirements, an

increasing number of vendors are producing Web-based network management products and an increasing amount of development is focusing on Web-based network management (Sridhar, 1997).

1. Universal Graphic User Interface (GUI)

The ease of the graphical user interface probably gives the biggest attraction of Web-based network management. Figure 4 is an example of an interface developed by Hewlett Packard called HP NetMetrix. Any desktop user is familiar to the Web browser GUI, which allows a wide range of users and expertise to have access to the same information, unlike proprietary management platforms. Although proprietary management platforms can present management information in a graphic manner, the software is still complex requiring much training and expertise in network management knowledge. The wide array and availability of Web browsers give an easy, cheap and common solution for managers to access network information. New improvements and proposals in WWW technology happen faster than users can keep up with. However, if network management is going to take advantage of improving capabilities of the Web, then it's logical to use the Web as a major tool.

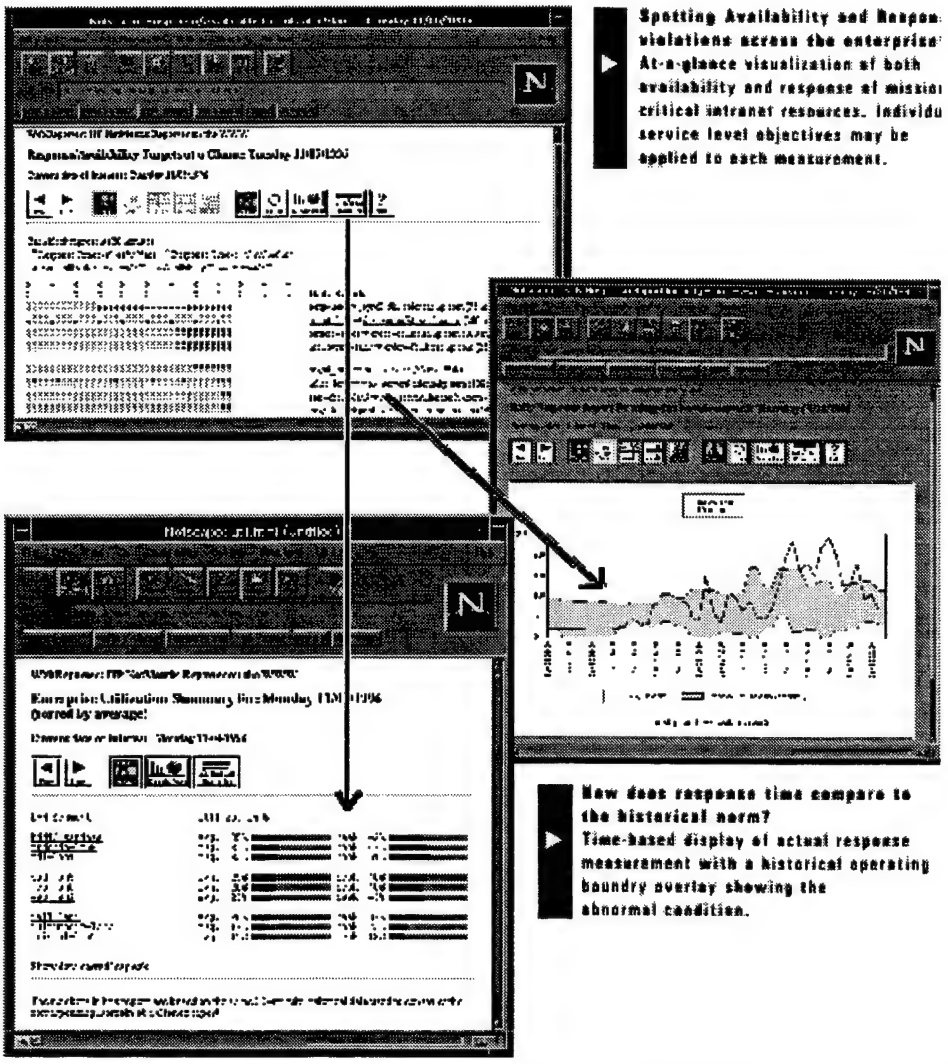


Figure 4. Example of a Web-based Network Management Interface. From Ref [HP].

2. Inexpensive Solution to Present Information

Traditionally to view information from an NMS, managers had to have access to powerful and expensive workstations. Products such as HP Open View require a lot of power to operate and usually require powerful and relatively expensive machines such as Unix workstations. Using the WWW allows managers and their organizations to choose what kind of architecture will dictate network management and not the other way around.

Although an enterprise network manager may not manage thousands of nodes on a PC, information can be displayed on PCs and a wide variety of other machines due to common protocols. This allows users from all levels of management to view network information that may be pertinent to them.

3. Protocols For Web-based Network Management

HTTP is obviously the protocol used for Web browsers based on TCP/IP. However, HTTP does not replace such network protocols as SNMP and CMIP. A common way to present management information is to imbed SNMP or CMIP within HTTP. This can be accomplished by (Deri, 1996):

- Extending standard HTTP servers.
- Creating a proxy application, which allows SNMP or CMIP protocol requests using HTTP.

a. Java Management Application Programming Interface (JMAPI)

The Java management Application Programming Interface (JMAPI) standard supports SNMP and is based around the Java programming language, which is quickly becoming a widely accepted WWW standard. Basically, JMAPI allows managers to take advantage of the same extensions and capabilities of Java (NRaD code 80, 1996).

b. Web-based Enterprise Management (WBEM) Architecture

A second proposed standard is to merge SNMP with HTTP known as Web-based Enterprise Management (WBEM). The elements of WBEM are (NRaD Code 80, 1996):

- HyperMedia Object Manager (HMOM): a data model to incorporate different information sets.

- HyperMedia Management Schema (HMMS): a data description for representing the managed environment.
- HyperMedia Management Protocol (HMMP): a communication protocol using HMMS, over HTTP.

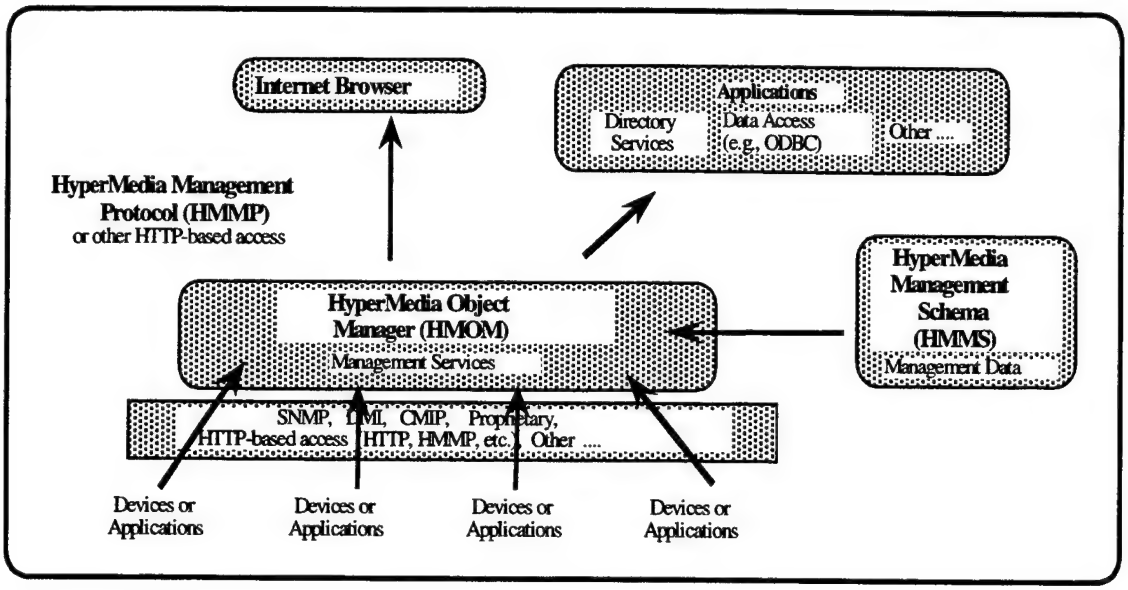


Figure 5. HyperMedia Management Architecture. After Ref [NRaD code 80].

4. Future Implications of Web-based Tools

Although the popularity of Web-based network management tools will grow, it probably will not replace standard network management tools. The functionalities of complex platforms such as HP Open View can not be duplicated on inexpensive hardware such as PCs. That is quickly changing. PCs are becoming more powerful and complex and there are certain network management tools available for PCs. However, powerful workstations are still required to handle the complexities of today's enterprise management. Web-based tools are also limited to the capabilities of the interfaces, where Network Management Systems allow managers to specifically obtain or manipulate the desired information by simply typing the required data sets. A current popular practice is

to integrate both tools in one environment. Web-based interfaces can supplement the Network Management System by allowing managers to access information in another format on top of such products as HP Open View by simply selecting an option in Open View's drop down menu.

IV. AUTOMATED DIGITAL NETWORKING SYSTEM (ADNS)

A. INTRODUCTION

The Navy's Automated Digital Network System (ADNS) provides a means for ships to centralize and automate the operation of multiple independent radio communications systems into an efficient communications network. ADNS provides connectivity for transmitting bits (which may represent voice, video or data) creating a seamless ship to ship and ship to shore communications network. By managing all of the radio assets within one system, ADNS creates a reliable multiple path communications network. This network is essentially a radio-based Wide Area Network (Radio-WAN). See Figure 6 (Casey, 1997).

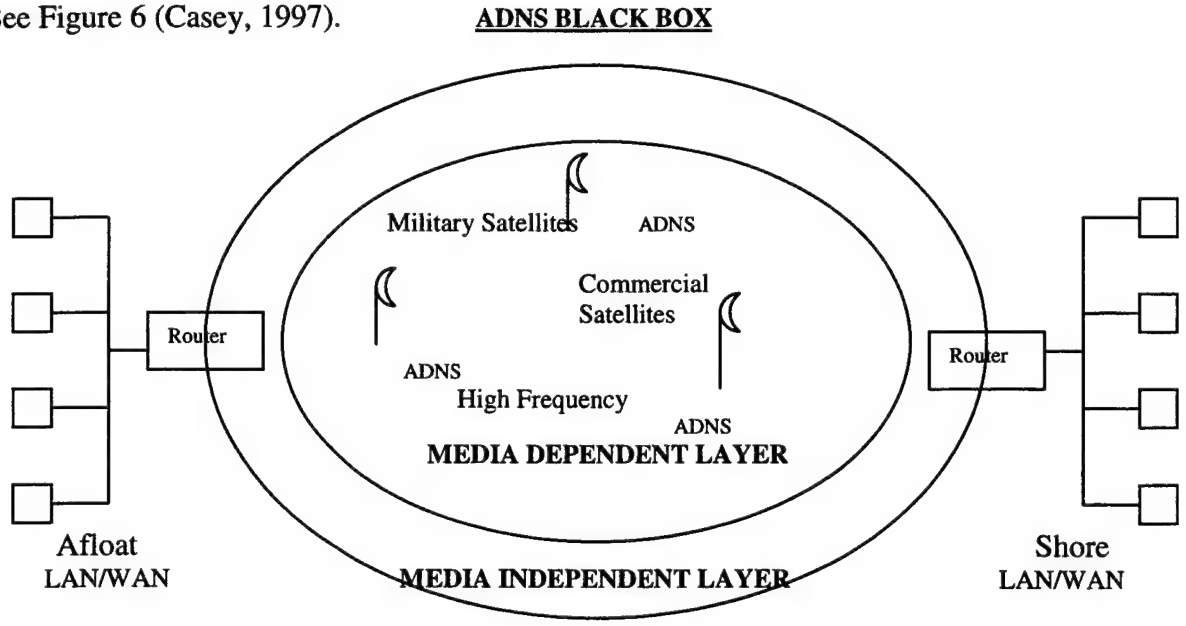


Figure 6. Large View of ADNS in an Internet Environment. After Ref [Casey].

Although currently a Navy specific installation, ADNS is like any other LAN/WAN Internet connection utilizing commercial products. Applications need only adhere to the established Internet protocols which ADNS has adopted. This allows a sense of transparency of applications to ADNS. It is also an open-ended system that

allows for future expansion. ADNS allows a plug and play like addition of radio links in a process completely transparent to the user.

For example, if an additional RF link is to be added, all that is required for that link to be compatible with ADNS is a Channel Access Protocol (CAP). This will be explained in further detail.

B. WHAT IS ADNS GOOD FOR?

A group of platforms, linked by ADNS, create a radio-based packet-switched WAN. By using existing Internet technology and open standards users of ADNS have seamless transparent access to the Internet. Using a load balancing concept ADNS spreads traffic equally across the appropriate radio links such that the available capacity is the sum of all the links. ADNS does not provide additional bandwidth instead it multiplexes the bandwidth that is already available.

There has recently been an insatiable demand for Internet access in areas never previously deemed necessary and although Internet technologies are relatively new, limitations are being experienced on traditional wire/fiber transmission paths. The primary purpose of wireless data transfer is for communications with mobile platforms. This capability already exists in various forms. However, ADNS provides a robust means of choosing the most efficient set of paths to transfer data in a way that is transparent to the user. It allows existing stovepipe systems to be integrated into one common data transmission network. When linked with a fixed shore site, to provide wire/fiber connectivity, this network becomes, in essence, a mobile extension of the Internet.

C. WHAT DOES ADNS DO?

A mobile platform can be thought of as a roaming Local Area Network (LAN). What existed onboard U.S. Navy ships prior to ADNS was a potpourri of different LANs and radio systems. If data was to be transferred to and from a ship, a different medium was used for each application such as high frequency (HF), ultra high frequency (UHF), or super high frequency (SHF). ADNS allows platforms with more than one transmission path to integrate these different systems via one black box (ADNS), which then distributes data throughout the different paths in the most efficient manner. This method is desirable for several reasons (Casey, 1997).

1. Load Sharing

If one or more transmission paths fail or are congested, ADNS can redirect data flow to open channels, which leads to an increased quality of service (QoS). ADNS can distribute data flow much more efficiently than the present stovepipe system. For example, a video teleconference (VTC) often inundates bandwidth, leaving other applications looking for an open transmission path. Other applications such as e-mail can be redirected to less congested channels instead of being stacked in a queue, waiting for transmission.

2. Cost Effective Bandwidth

ADNS can direct data from different applications through desired transmission paths. This can be done to preferentially use the most cost-effective means for data transfer.

3. Leverages the Existing Internet

Another big appeal for ADNS, and one of the main reasons why the Navy has developed it, is that ADNS ties together the existing stovepipe communications architecture. There is no need to create a brand new infrastructure. Existing organizational LANs can be connected to ADNS and have access to the full range of communications assets available to that unit.

4. Flexibility

The use of open protocols and Commercial off the Shelf (COTS) hardware creates a very flexible system. Modifications or additions to the shipboard LAN have no effect on ADNS. By using IP routers as the interface between ADNS and the shipboard LAN modifications on one side of the router are transparent to the other. Adding a new radio system is not much more complicated than adding a new circuit card.

D. HOW DOES ADNS WORK?

The easiest way to visualize how the system works is through an example. Suppose that a user on a ship at sea wished to transfer a file to another user on a different ship. Let us also assume that both users' computers are connected to their respective shipboard LANs. When the originating user is ready to send the message he simply clicks on the appropriate button to send the message on its way via the ship's LAN (Figure 7).

The size of most data files will necessitate their being broken into multiple IP datagrams. The router, processing each datagram independently, uses the Open Shortest Path First (OSPF) protocol to determine the best path(s) to reach the destination. If there are multiple equal cost paths the router will balance the load amongst them. Similar to a

packet switched network a single message may be routed via multiple paths. The router then forwards the datagrams to ADNS.

ADNS prioritizes, queues and transmits the datagrams on the selected radio system. The transmitted datagrams transit the Radio-WAN much the same way as in a packet switched network. At the destination there is a mirror image of the transmitting site. Arriving IP datagrams pass back through ADNS to the router and onto the LAN where they are received and reassembled at the destination host (Casey, 1997).

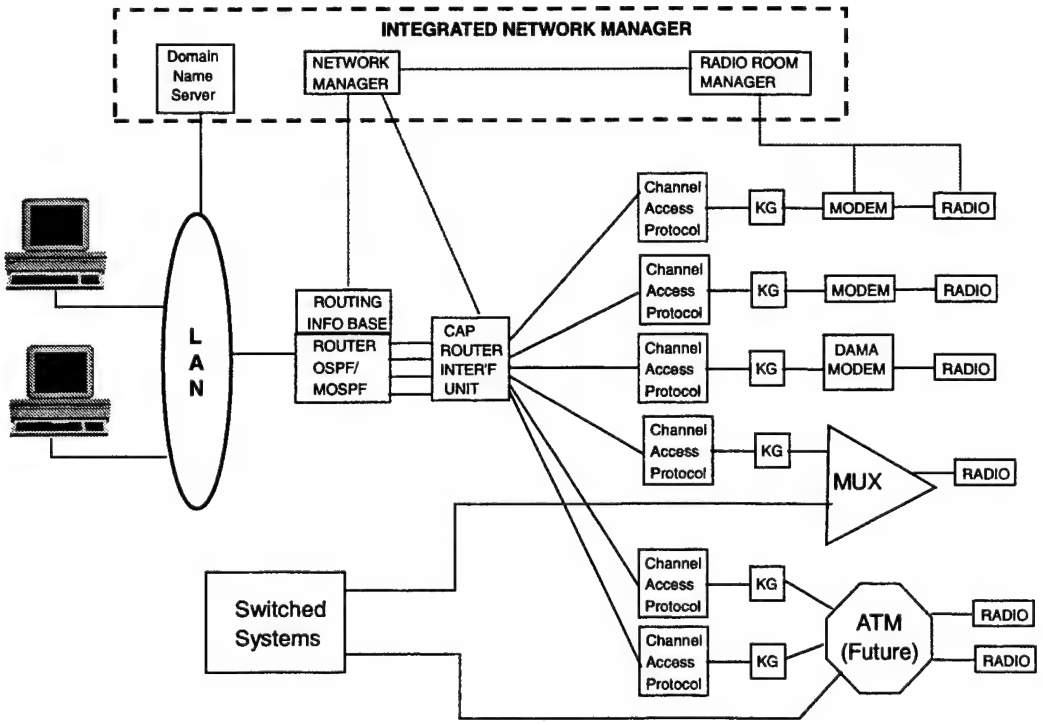


Figure 7. ADNS Configuration. From Ref [Casey].

This example described the transmission of one message to one destination via a single RF path. To understand the system's true potential, envision multiple ADNS capable platforms communicating simultaneously from multiple applications via multiple RF paths.

E. ADNS ADVANTAGES

1. Removing Humans From the Loop

In current naval communication systems, messages are generated on personal computers or workstations. These messages are transmitted via LAN, (or by use of magnetic media such as floppy disks where no LAN exists), to the communication center. The messages are then processed by technicians and transmitted. This process introduces time delays ranging from minutes to hours. ADNS eliminates the need for human processing of messages by establishing a direct connection from any node on the LAN, through the transmitter, to the receiver at the intended destination. The result is complete automation of the transmission process, with total elimination of any handling delays caused by human interaction.

2. Load Sharing

Most naval vessels maintain at least two operational communication channels at all times. The reason for multiple channels is that only certain types of information can be transmitted and received over each channel. This frequently results in one or more channels being completely silent, while another is backlogged with traffic. The Load Sharing Feature of ADNS was specifically designed to alleviate these backlogs by making more efficient use of all operational communication channels. This is accomplished assigning a "cost" value to each network. Message queues in each CAP are monitored and messages are routed evenly across equal cost circuits.

3. Optimal Use of Bandwidth

Network costs are assigned such that higher capacity circuits are assigned lower cost values. ADNS maximizes throughput by finding the lowest cost path for a message

to reach its destination. The combination of removing humans from the loop, load sharing and using the lowest cost paths discussed above results in a four-fold increase in throughput during peak traffic times. This is a direct increase in the bottom line throughput of the communications system without purchasing additional transmitters.

4. Communications Agility

ADNS provides the capability for two units that do not share a common communication channel to maintain communications. As long as each unit is operating at least one communication channel and at least one node on the network is operating both channels simultaneously, communications can occur. This process is completely transparent to the users, and occurs with no human intervention. This is analogous to Internet packet delivery. Few end systems share a common comms channel (that is, they are on the same network segment).

5. Transparency of Installation and Use

The installation of ADNS is totally transparent to the end users. It merely appears that a new router has been added to the LAN with links to many other LANs. There is no major LAN or transmitter reconfiguration that is required. Additionally, there are no major infrastructure modifications (cooling, ventilation, etc.) required and power requirements are modest.

6. Logistics

The entire installation is small and lightweight, allowing it to be installed in any unused space without impacting shipboard weight and balance.

7. Ease of Upgrade

Following initial installation, upgrading of ADNS is quite simple. Addition of new communication channels can be accomplished through the installation of the appropriate CAP cards. Adding capabilities to ADNS itself, such as installing successive builds as they become available, is as simple as downloading the new software. Router reconfiguration is a relatively simple matter as well.

8. Single Point for Communications Management

ADNS provides a single point for monitoring all communications, both incoming and outgoing. Prior to ADNS, monitoring all communications was much more difficult due to the lack of interconnection between stovepipe systems. Each of these systems had to be monitored separately. This monitoring capability is available locally via the local net manager's workstation, or remotely from the Network Operations Center.

9. Ability to Transmit All Types of Data

Essentially, ADNS transmits Internet Protocol (IP) datagrams from one router to another. It is the applications on these LANs that decode the datagrams and put the information contained in them to use. Therefore, ADNS can transmit text, graphics, voice, or video applications over existing channels, without the need for developing expensive new stovepipe systems to support each new application.

F. ADNS DISADVANTAGES

The high initial cost of an ADNS installation is a large obstacle to its widespread use. However, new technology, innovation, and mass production of ADNS should continue to drive costs down. The hardware used in an ADNS installation is COTS equipment but it is very implementation specific. It is unlikely that a unit will already

possess equipment that can be modified for ADNS in order to save money on an initial installation. However, future builds of ADNS are planned that will incorporate more readily available hardware.

G. ADNS OPERATIONAL DESCRIPTION

The behavior of the Radio-WAN created by ADNS is the same as a terrestrial WAN. The router on one platform still "talks" to routers on other platforms, but at a slower rate than if they were connected by wire or fiber. Some of the circuits used in the Navy's ADNS program, such as HF and UHF have transmission rates in the 2.4Kbps range. The insertion of the ADNS hardware and the RF transmission path is simply a conduit for creating a router based network. ADNS deals strictly with IP datagrams. Although some encapsulation occurs as a result of the handling process the underlying packets are not altered and thus the path between destinations is in essence transparent to the routers (Casey, 1997).

As discussed earlier, the router accepts outbound datagrams from the LAN and selects the best path for reaching the destination. The CRIU, which interfaces between the router and CAP, assigns a priority to outbound IP datagrams. Priority is inferred based on both the source application (logical port number) and the host (IP address) from which the message originated. At the CAP the message is placed in a queue to await transmission. Messages in the CAP queue are sorted by the priority assigned by the CRIU.

When the message leaves the CAP it passes through a cryptographic device. The standard Navy ADNS configuration operates at the secret high level of classification, thus all information entering the RF network is link encrypted. This (Casey, 1997):

- Conforms to existing practice.
- Provides resistance to AS spoofing.
- Provides limited content confidentiality/authenticity protection (because this layer of encryption is stripped off at each routing point). Although this provides protection during transmission it does not provide content security once the information passes through the cryptographic device at the receiving end.
- Provides opportunities for secure tunnels such as Unix Secure Shell (SSH) or Network Encryption System (NES), which deal with IP datagram encapsulation (IP datagrams inside other datagrams). These encapsulated IP datagrams are transmitted by ADNS in the same manner as any other IP datagrams.
- Does not affect applications that offer end-to-end security (e.g. secure e-mail). Similar to secure tunnels end system encrypted datagrams are unaffected by the presence of ADNS in the system.

After leaving the Cryptographic device the datagram passes through a modem and then enters the transmitter. Once it leaves the ship the message begins traveling via the predetermined path to its destination. Upon arrival at its destination the datagram, traveling through a mirror image of the originating system, terminates at the host specified in the IP header.

1. Routing Protocols

ADNS uses three different routing protocols. The primary reason for using these algorithms was that the specifications for all three are in the public domain.

a. Open Shortest Path First (OSPF)/Multicast OSPF (MOSPF)

OSPF is used as the Internal Gateway Protocol (IGP) for routing within an AS. The specification for OSPF Version 2 is contained in Request For Comments (RFC) 2178. It is a dynamic protocol in that each router maintains a continuously updated database containing the status of all other routers in the same system. OSPF uses a lowest cost algorithm to determine the best path to send a message to its destination. Costs are determined based on metrics values assigned to the various transmission paths.

Multicast OSPF (MOSPF) is used for multicast within an AS. The specification for MOSPF is contained in RFC 1584. MOSPF uses the same lowest cost concept as OSPF except the lowest cost is determined with respect to the group.

b. Border Gateway Protocol Version 4 (BGP4)

BGP4 is used as the External Gateway Protocol (EGP) for routing between ASs. Specifics for BGP4 can be found in RFC 1654. BGP4 is not as dynamic as OSPF and makes its routing decisions based on predetermined routes. In ADNS, BGP4 will typically reside at the shore station in a system. Since BGP4 requires a more stable environment than OSPF the shore station is the logical choice.

2. Logical Organization

The naming and logical grouping of the elements in an ADNS network are based on the concepts established by the routing protocols used by ADNS. The basic unit of an OSPF network is an area. For ADNS a ship is typically considered an area. Certain shore installations will also be areas since the ships need an interface point with other shore based establishments.

A number of ships grouped together using OSPF create an Autonomous System (AS). A typical AS consists of a group of Navy ships with some logical connection, such as a common mission. A Battle Group is a typical AS. The emphasis in AS establishment is on mission and not location. The units do not have to be in the same geographic region to be in the same AS. At least one and possibly two or more shore communications establishments will also be a part of an AS to act as the gateway to other navy networks such as SIPRNET (Secret IP Router Network) or the Internet.

The combined network of RF systems creates the subnet backbone of the AS. Each subnet is a different RF system such as UHF Satcom, SHF Satcom or INMARSAT B. The router on each ship that interfaces with ADNS is established as an Area Border Router (ABR). Each ABR operates OSPF. Part of the data that is maintained in the OSPF routing tables are metrics for each subnet in the AS. In current ADNS installations, metrics values are assigned based on subnet capacity or bandwidth. Higher capacity subnets are assigned lower metric values. The values chosen for these metrics determine how the system performs load balancing and load sharing, as discussed below. Obviously since each router must maintain a dynamically updated table of every other router in the AS there is a limit to the number of routers which can be managed effectively. This is what drives the upper limit to the size of an AS.

The router that acts as the gateway between an AS and other ASs, WANs, or the Internet uses BGP4. The shore establishment usually performs this function since BGP4 needs a stable environment. The OSPF to BGP4 transition acts to hide the internals of the AS from the outside. Routers outside the AS don't need to know the specifics of all the routers inside the AS. They only need to know where the BGP4 gateway into the AS

is. Changing missions will prompt changes to an AS. Ships may need to transfer from one AS to another to support operational or training objectives. This dynamic reorganization requirement reinforces the need to shield the internal routing issues of each AS from the outside. Figure 8 shows a generic AS architecture.

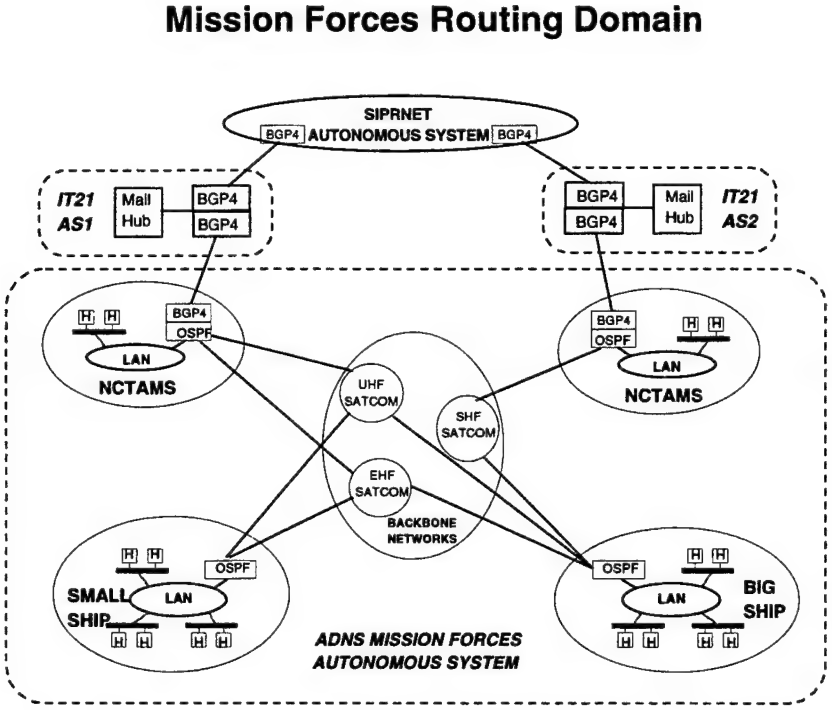


Figure 8. Generic ADNS AS Architecture. From Ref [Casey].

3. Key Features/Functions of ADNS

a. Priority

Several different methods for assigning priority to outgoing messages were evaluated during the ADNS implementation process. One obvious method, using the built-in precedence field in the IP header, was briefly considered. This idea was quickly discarded since no relevant applications currently use this feature of the IP header. Eventually, a priority scheme was implemented which assigned priorities of 0

(lowest) to 15 (highest). The two methods which proved most useful for assigning priority were based on source IP address (Host), or port number (Application).

This approach has the same advantages and drawbacks of a firewall which uses the same data to make its filtering decisions. The advantage is its practicality. The disadvantage is that it's rather crude and, at the moment requires manual configuration of the router's routing table.

(1) Priority Tables. The CRIU maintains two priority tables. The Source IP table contains the IP addresses of hosts on the associated LAN and the priority which they have been assigned. There are no default settings for this table. If a host is to have an associated priority it must be entered into the table. This table is filled in manually by the local ADNS Manager during initial system configuration and can be updated at any time. The Source IP table contains space for up to 40 entries.

The second table maintained by the CRIU is the Port priority table. It contains the dedicated port numbers used by certain applications and the priority that has been assigned to that particular application. Just as with the Source IP table above, there are no default values, priorities must be entered manually, and it contains space for up to 40 entries.

(2) Determining Message Priority. The CRIU receives datagrams from the router. The CRIU determines the port number and originating IP address for each datagram and assigns priority based on entries in the Source IP and Port priority tables. Here, a conflict may arise. If the Source IP priority table assigns a certain priority to a particular datagram and the Port priority table indicates a different priority for the same datagram, priority assignment will be made on the basis of Source IP

address. This allows priority based primarily on host, and secondarily on application should the host have no assigned priority. If neither the host nor the application have an assigned priority, the CRIU assigns a default value of priority 4. Once assigned, the priority is placed in the IP datagram header and the entire IP datagram is passed to the CAP.

(3) Message Transmission. Following Assignment of priority, the IP datagram is forwarded to the appropriate CAP, where it is entered into one of 16 queues based on priority. Datagrams are assembled into transmission units, each of which can contain up to 64 IP datagrams. The size of the transmission unit depends on the capacity of the link. Lower capacity links will have to utilize lower transmission unit sizes. The CAP builds a transmission unit by removing datagrams from the queues in order of priority. Datagrams are removed from the highest priority queue first, until it is empty. Datagrams are removed in sequence, continuing down the priority queues until the transmission unit is complete or all queues are empty. The transmission unit is sent from the CAP to the corresponding RF transmitter and the process is repeated.

b. Load Balancing

Load balancing is the sharing of transmission load equally among different subnets. When the router selects a transmission path it does so based on the metrics assigned to that RF system. OSPF metrics are based on link capacity, with links having similar capacity being assigned identical metric values. If multiple CAPs have the same metrics values then the router will balance the load evenly by alternating between those CAPs. For load balancing to work effectively the sharing must be done among systems of equivalent capacity. Consequently, when assigning metric values to RF systems it is

important that only networks of like capacity be assigned the same values. For example, if a ship is operating two active subnets, HF (which operates at about 2.4Kbps) and SHF (which operates at about 64Kbps) assigning the same metric values to each would overload the HF circuit. The router would divide the load equally between the two, not proportionally. During periods of high traffic density the SHF link could handle the load more effectively than the HF link, which would become backlogged with data.

c. Congestion Control

As described above, each CAP maintains separate queues for each priority (0-15). Should one of these queues become full, the CAP does not provide any overflow queue so additional datagrams with this same priority will be dropped. In order to prevent this situation from occurring, the CRIU monitors the CAP queues and either starts load sharing or issues a Source Quench command.

Each queue in a CAP is allocated a certain queue size to store IP datagrams prior to transmission. The CAP manages this queue space. The CRIU sets a queue threshold, slightly smaller than the queue size, to use as a benchmark to determine if congestion of the queue exists. The gap between the queue threshold and the maximum queue size provides a buffer to allow action to be taken before the queue becomes full and datagrams start being discarded. These queue thresholds are pre-determined and entered into the CRIU by the local ADNS Manager. The congestion identification function operates in the following sequence. The CAP generates a queue report, at intervals specified by the queue report threshold. This report captures the actual queue levels and sends them to the CRIU. These levels are compared to the queue threshold for each queue. If any queue level is greater than the queue threshold, then a

congestion condition exists in that queue. The macro behavior of this arrangement is very similar to congested routers in a conventional Internet so TCP, including the Karn and Nagel algorithms, will work without change.

(1) Load Sharing. One of the key features of ADNS is its ability to share the traffic load over available subnets. In current Navy circuits, a situation frequently occurs in which one communication channel is overloaded while another is completely idle. The load sharing feature of ADNS alleviates this problem by shifting some of the congestion to the idle channel, thereby increasing throughput and shortening communication system delays. This differs from load balancing in that balancing distributes traffic over channels with similar metric values before congestion occurs. Sharing distributes traffic over similar cost channels because a congestion condition exists.

(a) Restrictions. There are two restrictions on the use of load sharing. First, the traffic being shifted to an alternate channel must be unicast traffic only. Multicast applications introduce a level of complexity that causes diminished returns, making it not worth the effort to attempt to load share using multicast applications. Second, load sharing is only feasible between subnets whose bandwidths are in the same range, meaning they share a similar time delay. Thus, possible opportunities for a load sharing situation are between UHF and EHF, or between SHF and Challenge Athena.

(b) Implementation. The load sharing process begins when the CRIU determines that a congestion condition exists on a subnet in one of its associated CAPs. The CRIU then scans all other compatible (those with similar delay

times) subnets to determine if a path from origin to destination exists. If another subnet does exist with a path from origin to destination and no congestion condition exists on this subnet, load sharing commences.

(2) Source Quench. When congestion is determined to exist in the CAP queue for priority n, the CRIU issues a Source Quench ICMP command. This command stops the generation of message packets for all applications and hosts with priority n or less. Assuming compliant TCPs this Source Quench command has been pre-set to remain in force for five seconds. At the end of five seconds, transmission from the affected hosts and applications resumes automatically unless or until another Source Quench command is issued. It should be noted that all applications and hosts require some sort of flow control to ensure that during Source Quench conditions, packets are not discarded but rather stored for transmission when the Source Quench has timed-out.

d. Transmission Control Protocol (TCP) Duplicate Packet Transmission Problems

One of the major early setbacks to implementing the ADNS architecture was solving the problem of TCP duplicate transmissions when initially establishing a TCP connection. ADNS causes the LAN gateway router to act as if it is hard-wired to other routers on other LANs. Thus the router expects to encounter minimal delays (less than 0.5 seconds) in receiving acknowledgments to its TCP packets being sent. In reality, these TCP packets are being transmitted over RF links to distant LANs. The minimum acknowledgment time for a 1500 byte packet over a 2400 BPS connection is in the neighborhood of 5 seconds. When TCP hasn't received packet acknowledgment after 0.5 seconds, it re-transmits the packet. If acknowledgement is still not received after an

additional 1 second, TCP retransmits the packet again, and again after 2 seconds, 4 seconds, 8 seconds, and so on. Under optimal conditions, a 1500 byte packet will be sent 4 times over a 2400 BPS connection. The end result is the use of 6000 bytes to transmit 1500, an efficiency of 25%.

A practical solution, and the one implemented in ADNS, is to design the CRIU to discard duplicate TCP packets before they are transmitted over the RF link. This is accomplished by the use of a table for each subnet that contains the TCP sequence number and time-stamp indicating when the packet was received by the CRIU for transmitting. A TCP original packet and each duplicate packet sent will have the same TCP sequence number. When a TCP packet is received by the CRIU for transmitting, its TCP sequence number is examined. If this number already exists in the table, the packet is rejected. If this number does not exist in the table, it is added to the table along with its time-stamp, and the packet is passed along for transmission. Each subnet is assigned a TCP duplicate rejection time. If a TCP sequence number has been in the table for longer than the TCP duplicate rejection time, it is deleted from the table. The TCP duplicate rejection time has a default value of 10 seconds. This provides for transmission of the original TCP packet followed by a 10 second delay for acknowledgment. If none is received, the packet is allowed to be retransmitted followed by another 10 second delay. This time delay can be modified by the Local ADNS Manager with respect to the latency of the link for optimum performance.

H. ADNS INTEGRATED NETWORK MANAGEMENT

Network management of ADNS is based on SNMPv1 standards. There are no proprietary Navy protocols to confront, thus allowing the use of standard network

management tools and practices. Most of the objects to be managed (hosts, routers, etc) will have agents attached and MIBs will be written for any unique objects such as the CRIU or CAP. The Navy will adopt a standard, commercial Network Management System (NMS) to provide the foundation for network management. However, there are Navy-specific concerns, such as command and control relationships, which impact network management. For these special requirements, the Navy will create special applications and concepts to the NMS. This section gives a broad description of how the Navy intends to manage ADNS.

Network management of naval nodes is similar to managing shore-based nodes. The fundamental concepts are the same. However, the mobile nature of the nodes makes managing shipboard nodes more difficult and the fact that they are combatants makes network management more important. Just as there is a military hierarchy there is one for network management in ADNS, where each level has different responsibilities. Network management is a vital portion of ADNS because the consequences of system errors or failures can directly affect combat effectiveness.

Integrated network management describes how the Navy will manage networks on a distributed basis all the way down to individual objects. They include, but are not limited to: general monitoring, statistic collection, status monitoring, traffic monitoring, trend analysis, network loading, network optimization, configuration control, system configuration, maintenance, problem identification, problem reporting, trouble documentation, system administration, and emissions control (PMW 176, 1997).

Network management of ADNS contains three different levels: the Local Control Center (LCC), Autonomous System Control Center (ASCC), and the Navy Operations

Center (NOC). The LCC will be responsible for networks at the local level, e.g. within an area (usually a ship). The ASCC will be in charge of networks on a regional level, having several subordinate Autonomous Systems. The NOC will be responsible for all ASCCs in a certain geographic area. This arrangement is consistent with the Navy's organization and its doctrine regarding distribution of authority. See Figure 9.

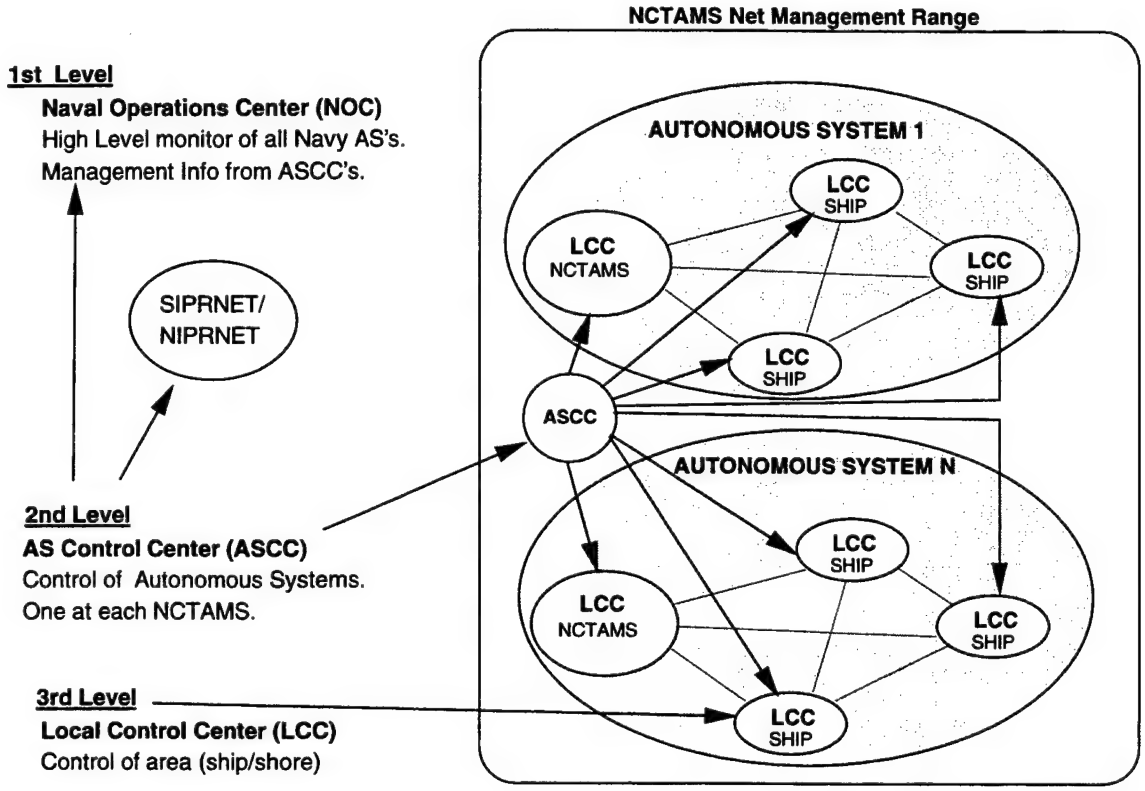


Figure 9. ADNS Management Architecture. From Ref [Casey]

1. Local Control Center (LCC)

The LCC is the network management center at every unit level. There is a local responsibility to monitor and maintain the status of all subnets at that unit. There are three components of an LCC: a Network Manager, Distributed Manager and a Communication Automation Manager.

a. Network Manager

The Network Manager is network management system software that is obtained commercially. The purpose of the network manager is basically to give the status of the network and individual objects. An example is the popular HP Open View Network Node Manager product (OV-NNM) which has been in the Navy Tactical Advanced Computer (TAC) contracts since 1991. It provides a topological map representation of a unit's network and shows the status of each object with the use of colors and shapes. However, human interaction is required to interface with the ASCC and the NOC for troubleshooting or maintenance. The specific functions of a Network Manager will be (NRaD, Code 80, 1996):

- Human machine interface
- Performance management
- Fault management
- Accounting management
- Security management
- Configuration management

The Network Manager will be used as the foundation for the Navy's Integrated Network Management System, where specific applications can then be added on to provide other management functions.

b. Distributed Manager

Distributed Management is an application that determines what is to be reported locally and what is to be reported to the ASCC and NOC. The Distributed

Manager has two mechanisms for discovering if any conditions exist that meet the criteria of its policy rules (NraD, Code 80, 1996):

- Notification from the Network manager
- Query from Distributed Manager to Network Manager

The specific functions of the Distributed Manager will be:

- Interpretation and implementation of policy
- Filtering of management information

Although commercial products can provide these functions, the distributed manager in the Navy context specifically describes the policy rules for the communication relationships between the LCC and ASCC.

c. Communication Automation Manager (CAM)

The Communication Automation Manager is in charge of the physical communication hardware and their related requirements. On a ship, they are functions typically related to the radio room. Duties include a communication plan implementation, circuit building, and circuit management. Three areas make up the Communication Automation Manager: the Communication Manager, Site Manager, and Equipment Manager. The specific functions of the Communication Automation Manager will be (NraD, Code 80, 1996):

- Security management
- Log Control
- Alarm reporting
- Summarization
- Attributes for representing relationships

- Objects and attributes for access control
- Usage Metering
- Test Management
- Event Report Management
- State Management
- Security alarm reporting
- Object management
- Bandwidth management
- Communication plan management
- Equipment control
- Site configuration management

The Navy specific application for these functions is the use of a remote management tool called the Communications Plan (COMMPLAN). The COMMPLAN will used to direct certain network management functions as described above. This is still mainly accomplished manually by a technician after receiving the COMMPLAN via hardcopy message. However ADNS will allow many of these requirements to be accomplished remotely and automatically via the COMMPLAN transmitted to the Communication Automation Manager. This concept can be applied to commercial industries where it is not cost effective to have the necessary network management expertise at every local site but can instead be centralized at one remote center.

2. Autonomous System Control Center (ASCC)

An ASCC monitors the operation of several LCCs. The Navy's configuration will use its regional shore communications master stations (NCTAMS) as ASCCs. The

ASCC will receive summary reports from subordinate LCCs. The exact nature of reporting from an LCC to an ASCC is still to be determined but will contain mission relevant information. Such reporting requirements can include (Casey, 1997):

- Readiness of communication to support the mission.
- Status of communication services.
- Status of hardware and software.
- Information about usage and reliability.

ASCCs can also give direction to LCCs regarding communications posture. This could include such items as prioritization of resources or equipment configuration changes.

3. Network Operations Center (NOC)

The NOC is the next level above an ASCC for reporting network management information. The NOC would basically monitor all nodes in a certain geographic location. For example the Navy has established a NOC in the Pacific and Atlantic regions. Although capable of monitoring detailed network management information, a NOC would be more interested on the overall status of ASCCs and LCCs.

4. Network Management Tools

To achieve the above network management requirements, a vast array of tools are available to all levels of management and maintenance personnel. However, each tool comes with their own training requirement. Therefore the total cost of ownership must be taken into consideration against their utility. The basic tool for monitoring the network is commercially available Network Management System software. Another tool available for the goal of transparent and affordable network management is software that

is capable of remote monitoring and maintenance. These can also be available commercially or can be developed to be mission specific. There are always emerging tools on the horizon for new technologies. However, one of the primary reasons why network management techniques lag behind new network technologies is that time is needed to see which technologies will become established as industry standards. ADNS will manage objects primarily through SNMPv1 standards. That is not to say that ADNS can not adapt any emerging technologies that become industry standards, such as SNMPv2. However, SNMP has proved that it will be around for a long time.

a. Network Management System Software (NMS)

A commercial Network Management System software has been adopted for the foundation of the INM. Network Management System software allows for the basic functions of monitoring nodes and network status. As described earlier, many different types of enterprise management software are available commercially, such as the popular HP Open View Network Node Manager (OV-NNM). Although commercial software provides excellent monitoring tools, proprietary software is often required to achieve other network management requirements. Commercial Network Management System software offers a fairly inexpensive solution that provides a solid foundation of network management tools. Additionally, to provide the flexibility desired throughout ADNS a COTS product is appropriate.

b. Third Party Applications

An attractive feature of a Network Management System such as OV-NNM is that third party applications can be integrated into it. Especially for organizations like the Navy, solutions to mission specific requirements can not be obtained off the shelf.

These mission specific add-ons must be developed independently and then integrated into the existing NMS. Proprietary equipment also requires some kind of integration with the NMS. Such things as configuration management software for specific objects must be obtained from the vendor. For example, companies offer software that can be integrated with an NMS to allow managers to remotely configure their hardware. Third party applications offer remote management capability. This is the whole purpose of enterprise management. It is very cost effective to centrally manage nodes rather than paying for the necessary expertise at every local level. Although there needs to be some human interaction at every level, full management capabilities are not required down to the local level.

ADNS is a good example of the need for remote management. Implementation of remote management over ADNS will allow managers to configure and manage mobile platforms from a central management location. This, in turn, allows the assignment of minimal personnel at the local level, thus saving on personnel costs. With such standards as RMON and SNMPv2, remote managers can access remote networks in a secure manner and troubleshoot or reconfigure the network. For example, if one transmission path fails, a remote manager can gain access to the system via a second transmission path and troubleshoot the system. The use of more than one transmission path allows the ability to continually manage LCCs and even ASCCs remotely through just one open path. Although ADNS has not adopted such standards as RMON or SNMPv2 yet, the technologies currently exist and can be readily integrated into ADNS.

I. HARDWARE

1. LAN

The LAN will typically be the existing shipboard Ethernet or FDDI network. Hosts on the network will run a wide variety of applications.

2. Router

The router is an IP router that acts as a gateway to the ADNS network. The router can be any commercial router capable of running OSPF

3. CRIU (Channel Access Protocol to Router Interface Unit)

The CRIU is implemented on a single board computer installed in a VME chassis.

4. CAP (Channel Access Protocol)

A CAP is also implemented on a single board computer mounted in the same VME chassis as the CRIU.

5. Cryptographic Device

Navy ADNS installations use the KG-84 for link encryption.

6. Modem

For each CAP there is a corresponding Modem that performs the analog to digital (inbound) or digital to analog (outbound) conversion of data passing through ADNS.

7. Connectivity Media

Each RF system (e.g. UHF Satcom, EHF Satcom or INMARSAT B) constitutes one network when considering all assets in one ADNS Autonomous System.

J. CONCLUSION

ADNS provides the means for the Navy to operate in a network-centric fashion. Because of this proliferation of networks especially on ships, network management

becomes critical to overall combat effectiveness. Although ADNS provides the technical answers for the Navy's network requirements, further solutions are needed in the area of how to manage these networks. Chapter V proposes one solution to use a Web-based interface to represent network management information relevant to different levels of Autonomous Systems in the Navy.

V. WEB-BASED MISSION-CENTRIC NETWORK MANAGEMENT PROTOTYPE TOOL FOR ADNS

A. MISSION-CENTRIC NETWORK MANAGEMENT

The previous chapter clearly shows the Navy heading in a network-centric way of conducting business. However, what is even more important is how the network will impact the unique roles and missions of the Navy (mission-centric network management). This emphasizes the role of network management as becoming increasingly critical, especially in the military's role of providing national and international security. Navy decision-makers, on all levels, are interested in managing some form of network management information. Lower level managers would be interested in controlling networks. Commanders would be interested in understanding the networks' effects on combat effectiveness and others can use the information for planning purposes. Network management concepts can be very complex and technical. Not all managers are interested, nor should they be, in the detailed data that can be provided by a Network Management System. However, what is of particular interest to Navy commanders and other decision-makers is what and how network management information is pertinent to their job, task, or particular mission. Such information can transform technical data (e.g. SNMP agents) into reports that impact the mission. A term to define such requirements can be labeled as mission-centric network management (Jacobs, Inchiosa, Gutman, and Barber, 1997).

Mission-centric network management describes the support that network-centric capabilities have on the uniqueness of Navy units. Navy units perform a wide variety of missions on shore, at sea, in the air, and under water. Each mission is unique and specific

as directed from higher authorities. With the relatively new capabilities of networks, especially on sea-going units, it critical that these networks help and do not hamper the missions assigned. The degradation of a network on a unit can cause a deficiency in combat readiness, which can have dire consequences. This needs to be understood less in terms of communication outages and more in terms of impact on mission capability. The goal of a network-centric approach in the military is to provide an increased ability in combat effectiveness. Therefore, it is highly desired to manage network information that is mission-centric.

1. Commercial Products Not Available for Specific Navy Requirements

Standard network management products are commercially available and are always being upgraded in capabilities and performance. However, because of the unique capabilities and requirements of the military, commercial products are not available for mission-centric requirements. Although there has been a big push recently to obtain commercial products off the shelf, this can not always be accomplished. Specific military requirements will always need tailored designs and applications built.

That is not to say commercial products should not be adopted for military means. Commercial products allow costs to be cut in terms of research, development, implementation, and other life cycle costs. If commercial standards such as SNMP exist, why not leverage these technologies where applicable to military requirements.

2. The Use of Commercial Business Practices

Although commercial products are not always available or entirely suitable for Navy specific requirements, successful commercial business practices can be adopted to increase efficiency. One of these commercial practices is using the Web in an Intranet

environment. Because of the Web's universal access and many other appeals, it is a great tool for the Navy to manage mission-centric network information. The use of Web-based technology allows Navy personnel of all expertise levels to view and manage information on a common and familiar interface. Web pages can be uniquely tailored to different unit levels such as an individual ship, battle group, or force to present different levels of mission-centric information.

B. WEB-BASED PROTOTYPE FOR MISSION-CENTRIC NETWORK MANAGEMENT

The descriptions of Web-based network management tools in Chapter III show the ability to manage objects directly from a Web-based management station. However the prototype in this thesis is a rough attempt to show what mission-centric views may look like in a Web-based interface. The Web pages are accessed via an ordinary Web browser, such as Nestcape, that interfaces with a commercial Network Management System such as Hewlett Packard's Network Node Manager (HP-NNM). In this prototype, HP-NNM manages objects on the network and would feed the status of the objects to the prototype via specially designed MIBs. The prototype would then use that information to present mission-centric network management information. Information transferred outside the Local Control Center (LCC) is not via HTTP but rather through the use of SNMP. SNMP uses little bandwidth, as compared to HTTP, so is much more cost effective. Outside managers (Autonomous System Control Center (ASCC) or Network Operations Center (NOC) level) will view Web-based information through the Network Management System interface (HP-NNM) just like the local level (Figure 10).

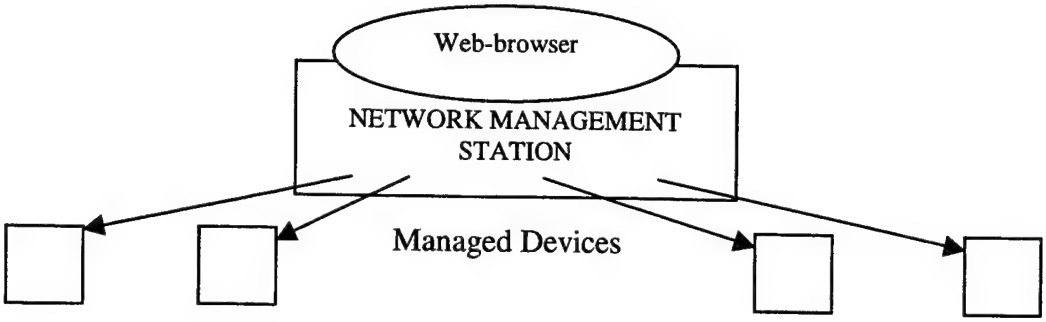


Figure 10. Prototype Layout at the Local Level

Prototype Web pages were designed to take an initial step towards the goal of using the Web for managing mission-centric network information. The Web interface will be designed to be accessible via an option in a standard Network Management Platform such as HP Open View Network Node Manager (HP-NNM). It will be used in conjunction with HP-NNM, since the prototype will obtain status information directly from HP-NNM. There are four colors to indicate different status levels of efficiency.

The colors are based on an algorithm that receives SNMP information from HP-NNM. The colors indicate an aggregate measure of objects on a network that respond to SNMP messages that affects a particular Local Control Center (LCC), Autonomous System Control Center (ASCC), or Network Operations Center (NOC). Certain objects will run applications affecting a certain mission area. If certain objects are not responding to SNMP messages, then the missions affected by those objects will be degraded.

For example, the top status level, which indicates that a particular node or function is totally up or 100% efficient, is shown by the color green. This means that all

the objects that affect that node are up and responding to SNMP messages. Yellow indicates a 75% efficiency rate. The algorithm to determine the color yellow indicates that the aggregate measure of objects affecting that particular node has a certain combination of objects responding to SNMP messages and a certain number not responding to SNMP messages. Yellow basically implies that on a certain node, a few objects are down. Orange indicates a 50% efficiency rate which indicates more objects are not responding to SNMP messages. Blue indicates 25% efficiency rate. Red means that the status of that node is totally down (no responses from any objects).

The prototype uses a sample of different Navy platforms (in this case arbitrary ships) and certain Navy applications that can be found on those platforms. These applications are used to accomplish certain tasks and missions. This list is by no means complete. It is an attempt instead, to demonstrate the ability to show the impact of mission-centric information in form of a Web interface. The ships used were picked arbitrarily and do not reflect actual ship architectures. The eventual goal would be, if this concept comes to fruition, to map any object that is managed via SNMP to a mission-centric view.

C. PROTOTYPE IMPLEMENTATION

The pages were designed using Microsoft Front Page which is an easy to use interface without having to type Hyper Text Markup Language (HTML) code. These pages were designed for the Naval Command, Control and Ocean Surveillance Center (NRaD) code D827's research and development in ADNS INM and are by no means complete. The examples shown in Appendix B are the current prototype pages which will continue to be refined and upgraded by NRaD code D827. The prototype applies to

the three different levels of ADNS network management: the Local Control Center (LCC), Autonomous System Control Center (ASCC), and the Naval Operations Center (NOC). The Web interface will have to be individually tailored to each LCC, ASCC, and NOC.

1. Interface for the Local Control Center (LCC)

Figure 11 is the web page developed to show mission-centric information of an LCC. The right frame is the main frame for the LCC. This can be treated as the LCC's main page. It can contain specific information about the LCC, but in particular, it can show the status of a mission that the LCC is to accomplish.

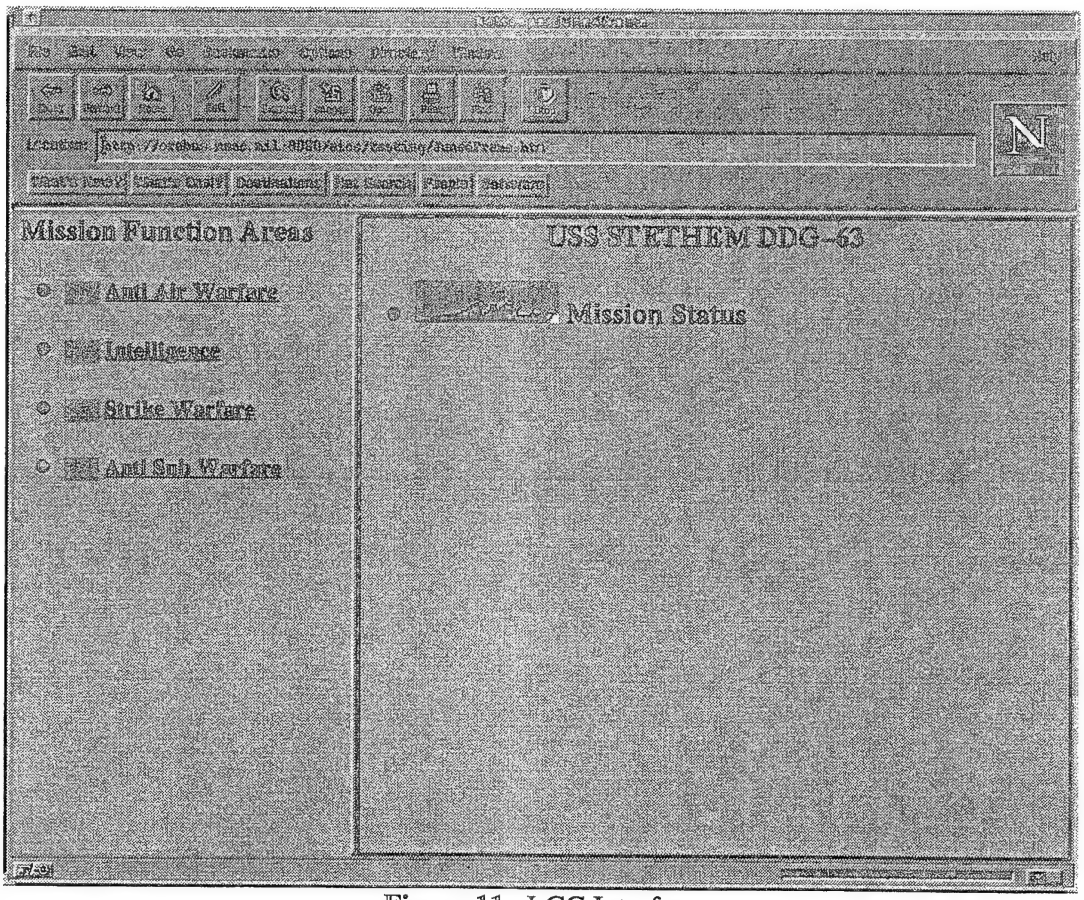


Figure 11. LCC Interface

The example used in the main (right) frame is the USS STETHEM, DDG-63. It shows an overall mission status of green. This means that because of the current efficiency of the networks onboard the USS STETHEM, the networks affect the entire ship's overall mission status to a 100% efficiency rating. What contributes to the overall mission status are the mission function areas of the ship.

a. Mission Function Areas

Mission function areas are specific missions a unit is able to perform such as anti-air warfare (AAW), anti-surface warfare (ASUW), or anti-submarine warfare (ASW). Therefore the overall mission status of an LCC would be determined by as an aggregate of the individual status of each mission function area. So the left frame in figure 11 shows the status of each mission function area of the USS STETHEM which contributes to the overall LCC mission status of green. The individual status of each mission function area can be determined by this structure.

The architecture is a hierarchical tree. At the top of the tree is the overall status of the LCC, which is the aggregate of the mission function area statuses. Below the top level is the status of the mission function areas of the LCC and below these levels are the individual components that contribute to status of the higher levels.

b. Mission Function Area Applications

The status of the of the mission function areas are determined by the status of applications used by the mission function area. For example, certain applications are required to carry out the mission of AAW. There are hyperlinks from the status of the Mission Function Areas Web frame to an applications Web frame that shows all the

applications that contribute to a certain mission function area like AAW. So if the AAW link in figure 11 is clicked, it will show figure 12.

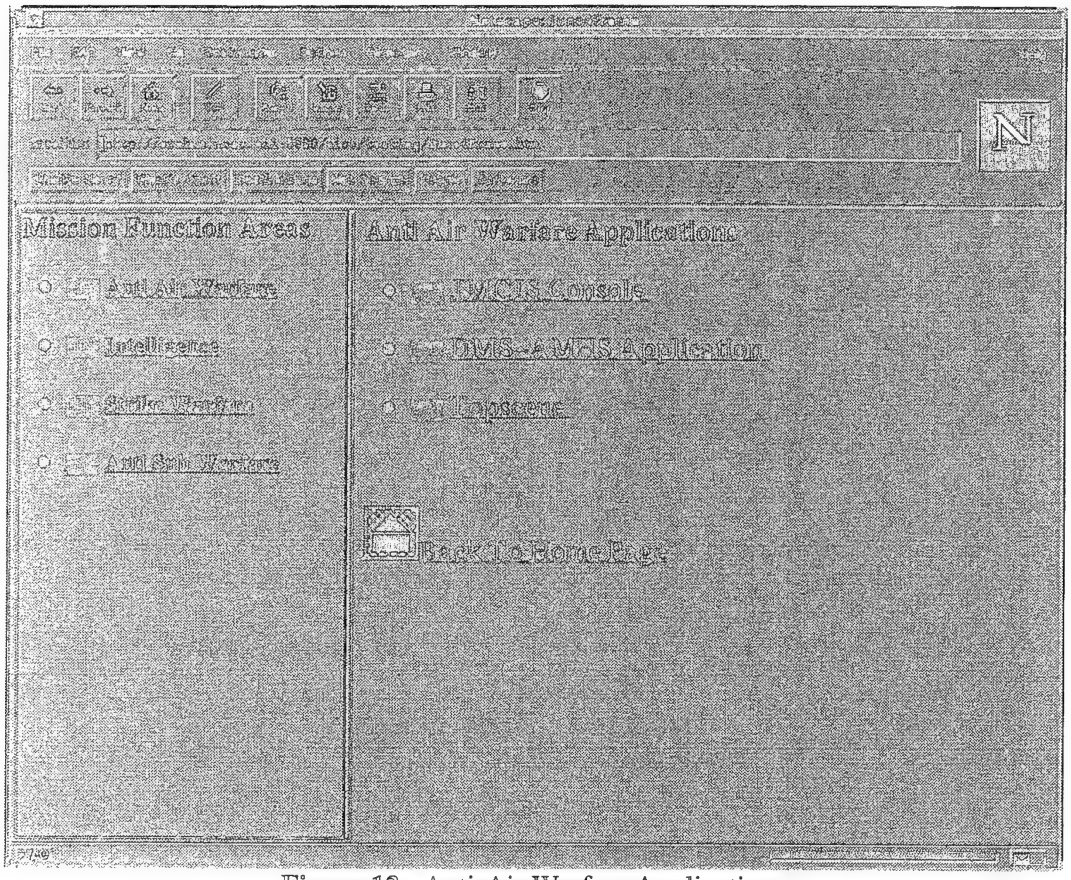


Figure 12. Anti-Air Warfare Applications

Figure 12 shows that JMCIS, DMS-AMHS, and Topscene contribute to the mission of AAW. It shows the individual status of each application. Each application is also a hyperlink to subordinate levels, which are the transmission resources of those applications.

c. Application Transmission Resources

Each application has a transmission resource to transmit and receive data. So if the JMCIS application status hyperlink is clicked, it will show the status of its

transmission resource (Figure 13). Figure 13 shows that the JMCIS application uses Ethernet and the status of the Ethernet.

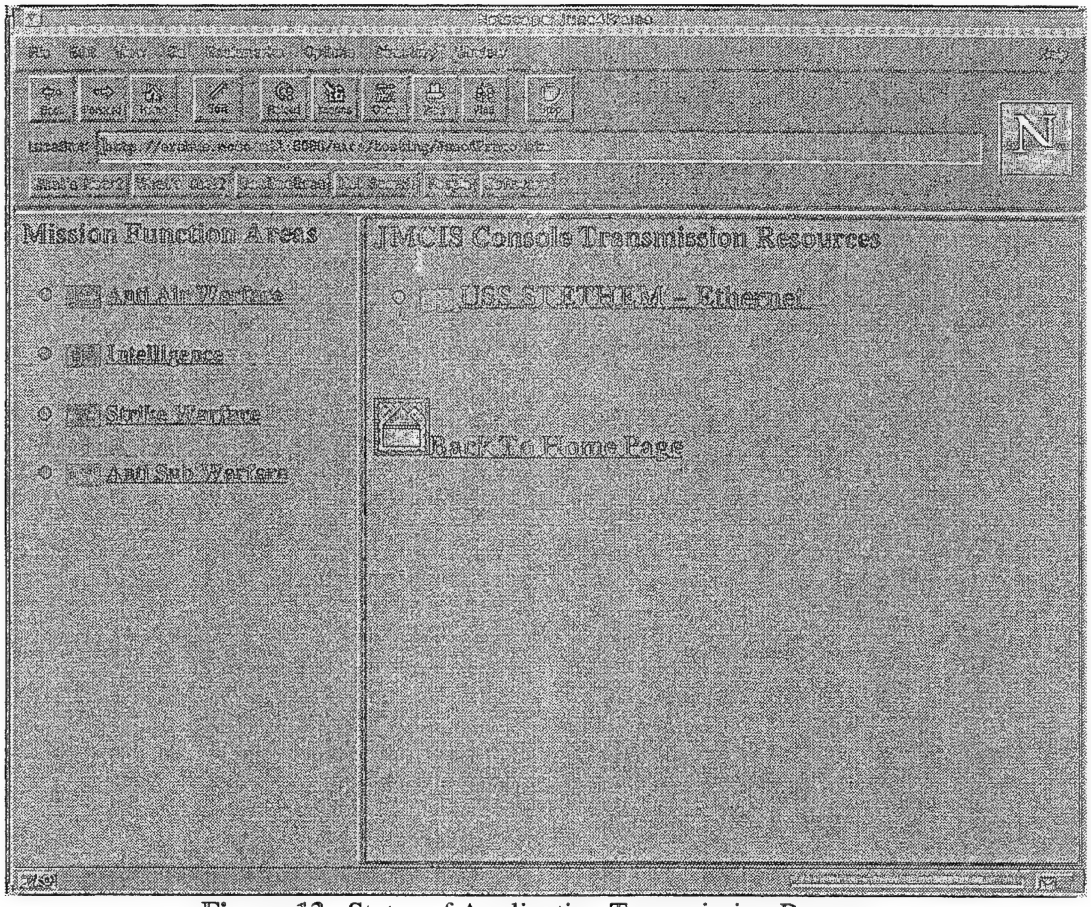


Figure 13. Status of Application Transmission Resource

d. Objects on a Transmission Resource

Transmission resources have many objects that are attached to it with different applications. In Figure 13, if the Ethernet status was degraded, it could be due to the status of any of the objects attached to the Ethernet backbone. So if Ethernet hyperlink in the Transmission Resource frame is clicked, it would present the Ethernet Equipment frame. The Ethernet Equipment frame shows all the objects attached to Ethernet and their status (Figure 14). This structure goes down one more level and shows the status of the ports of each individual object (Figure 15).

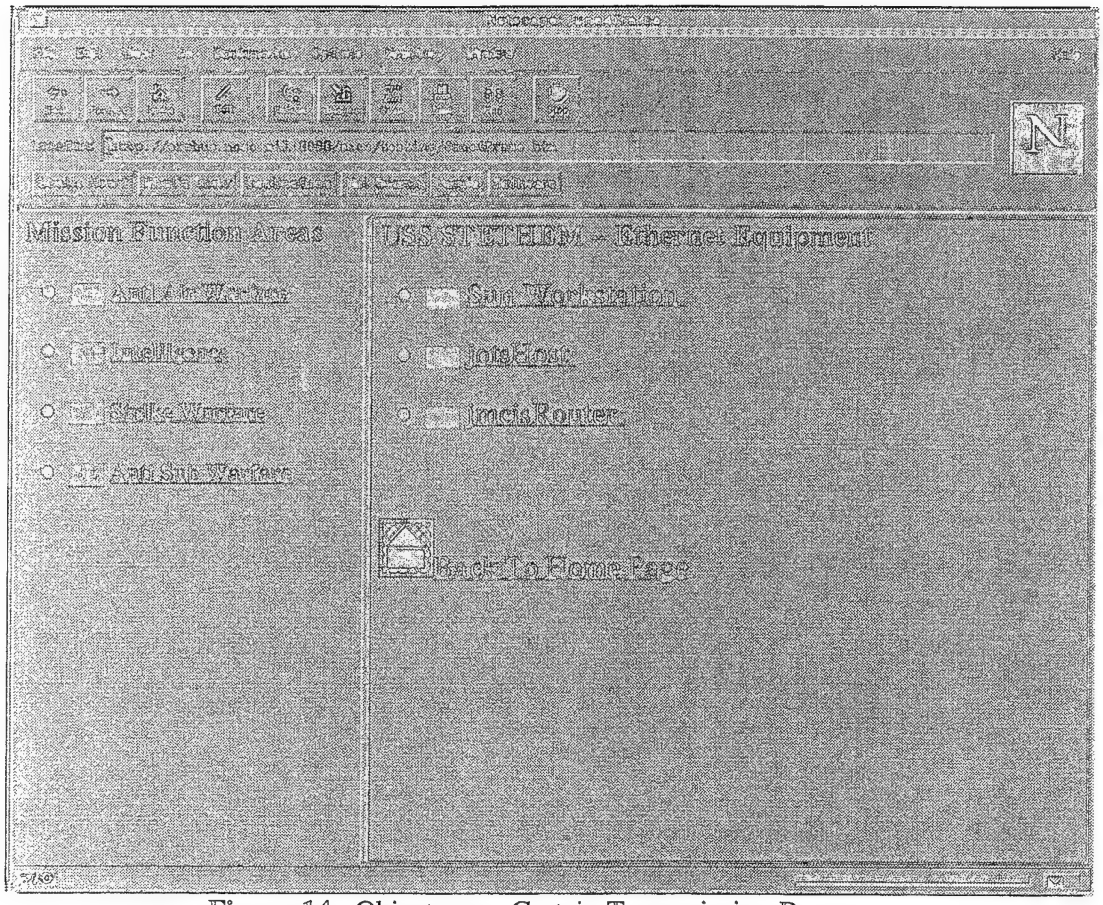


Figure 14. Objects on a Certain Transmission Resource

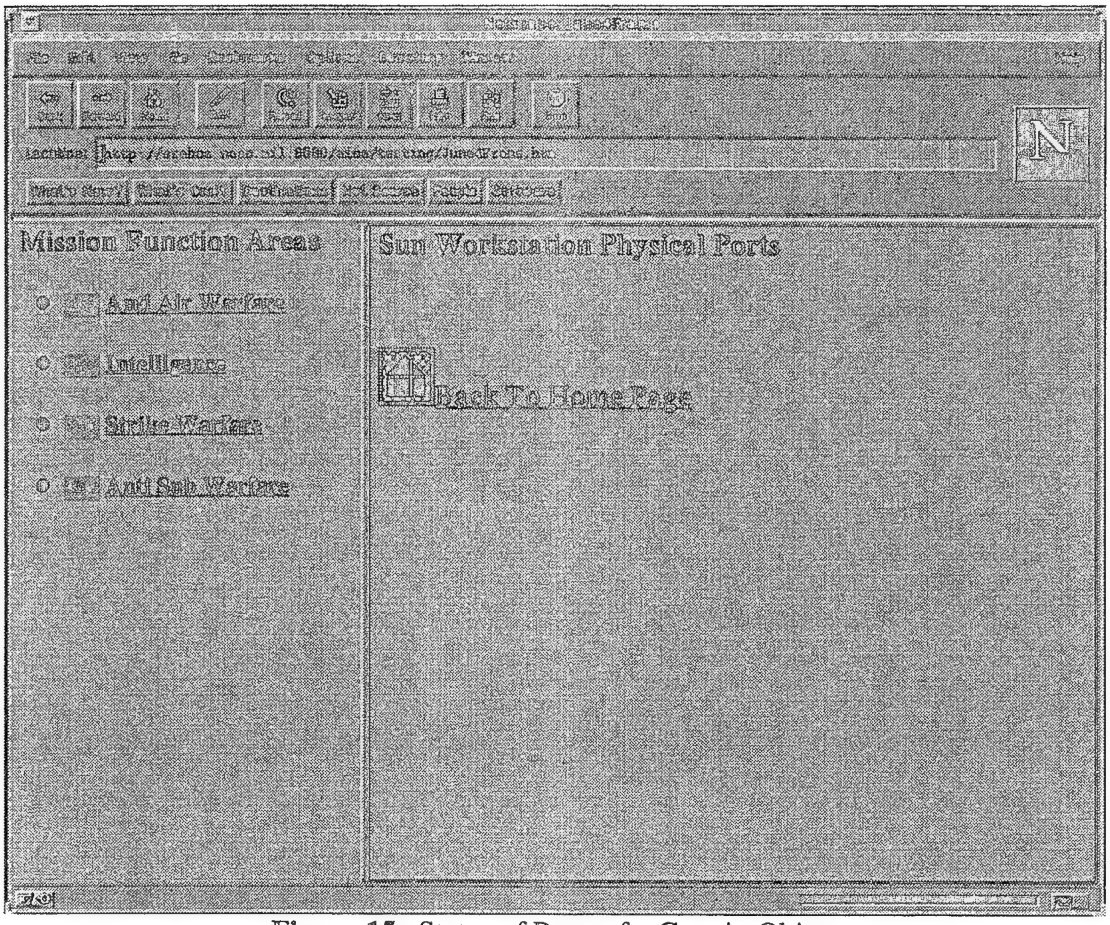


Figure 15. Status of Ports of a Certain Object

2. Interface for the Autonomous System Control Center (ASCC)

The ASCC interface is very similar in concept to the LCC interface. The ASCC is on a higher level of authority and would normally be in charge of a number of LCCs. The network managers onboard an ASCC would be interested in viewing the status of the LCCs that it is in charge of managing. So in a battle group example, the network managers would be interested in managing network information of subordinate units such as destroyers, cruisers, frigates, and submarines in the battle group. However, the ASCC still retains the capability of viewing it's own network information (LCC view).

Figure 16 is an example an ASCC interface. The right frame is the main frame and presents the overall mission status of the ASCC. There are hyperlinks of the mission

function areas, user applications and transmission resources. These hyperlinks show frames similar to the LCC frames that contribute to the different statuses of ASCC.

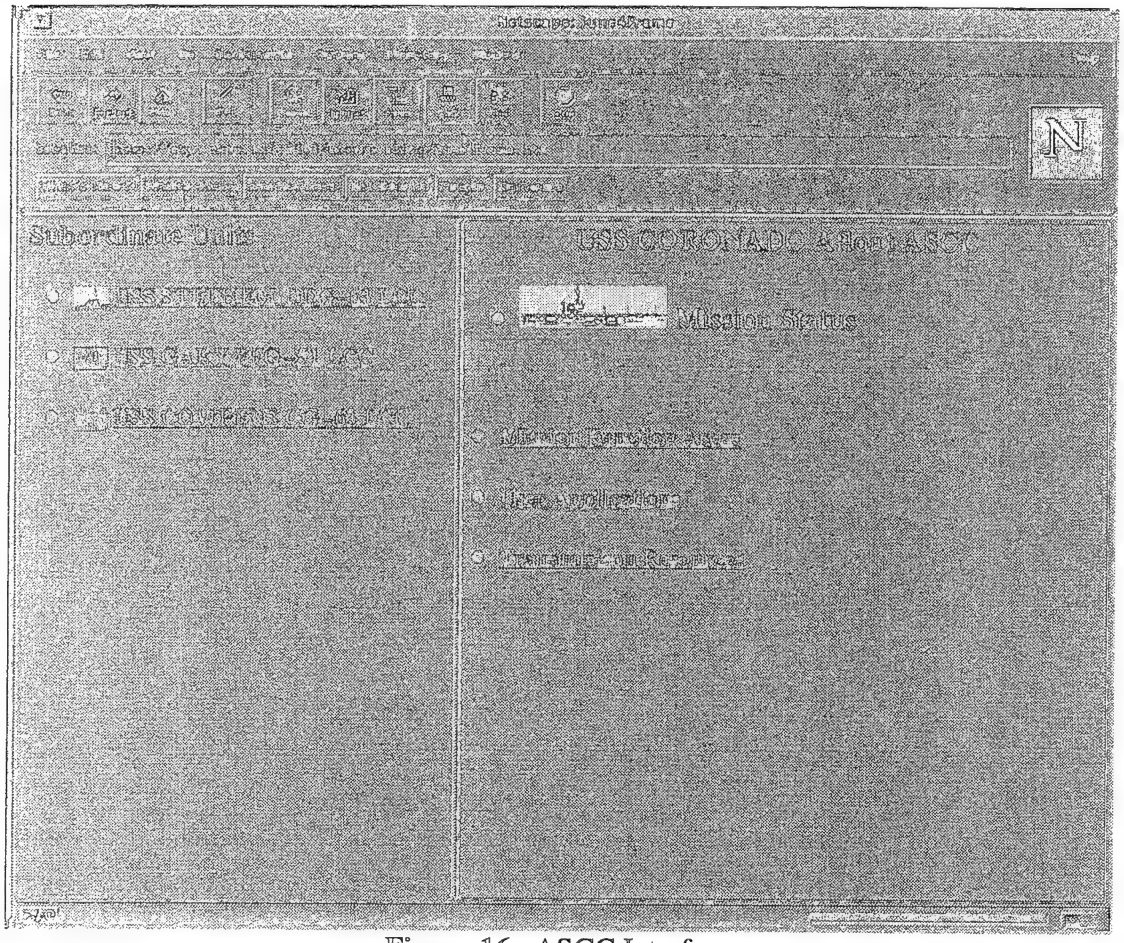


Figure 16. ASCC Interface

The left frame indicates which units are subordinate to the ASCC and their overall mission status. If the subordinate unit status hyperlink is clicked, it shows a summary frame of what is contributing to the overall mission status (see Figure 17). Notice however that the summary frame does not show the extensive amount of network information that one can obtain on the LCC interface. This is because the managers and decision-makers on an ASCC will only care about a higher level amount of information.

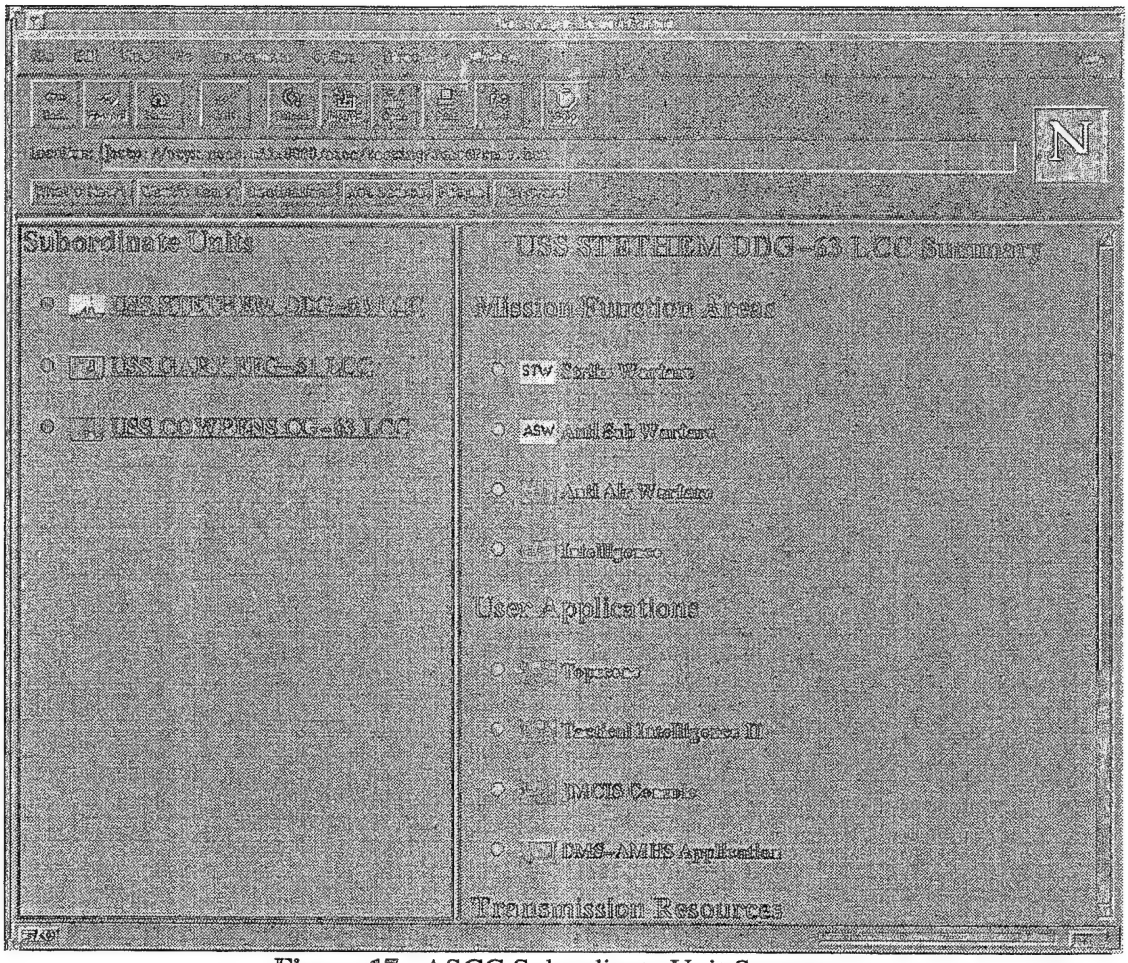


Figure 17. ASCC Subordinate Unit Summary

On the main frame of the ASCC, summary information about the ASCC, similar to the LCC interface can be obtained. In this particular prototype, summary information on the ASCC's mission function areas, user applications, and transmission resources are available. Figures 18 - 20 show these summaries.

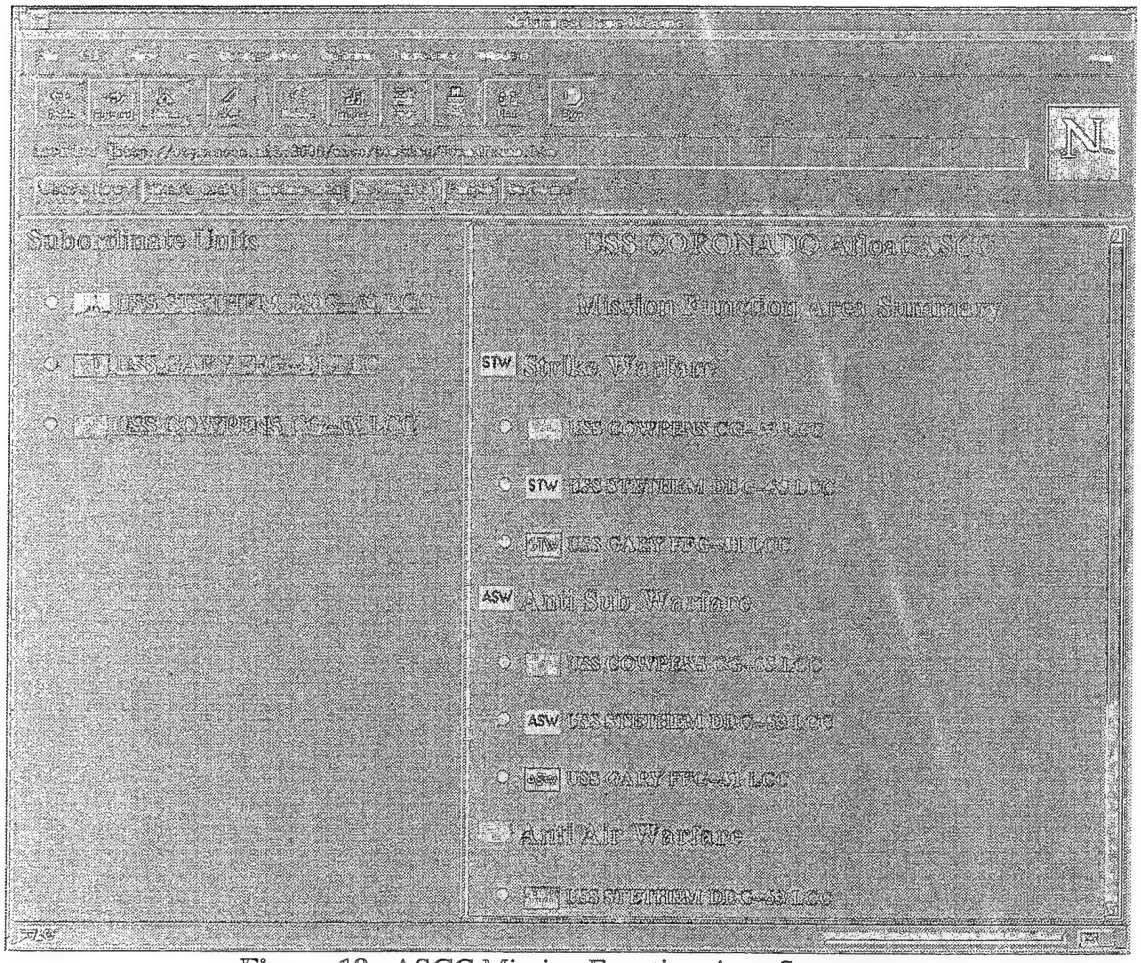


Figure 18. ASCC Mission Function Area Summary

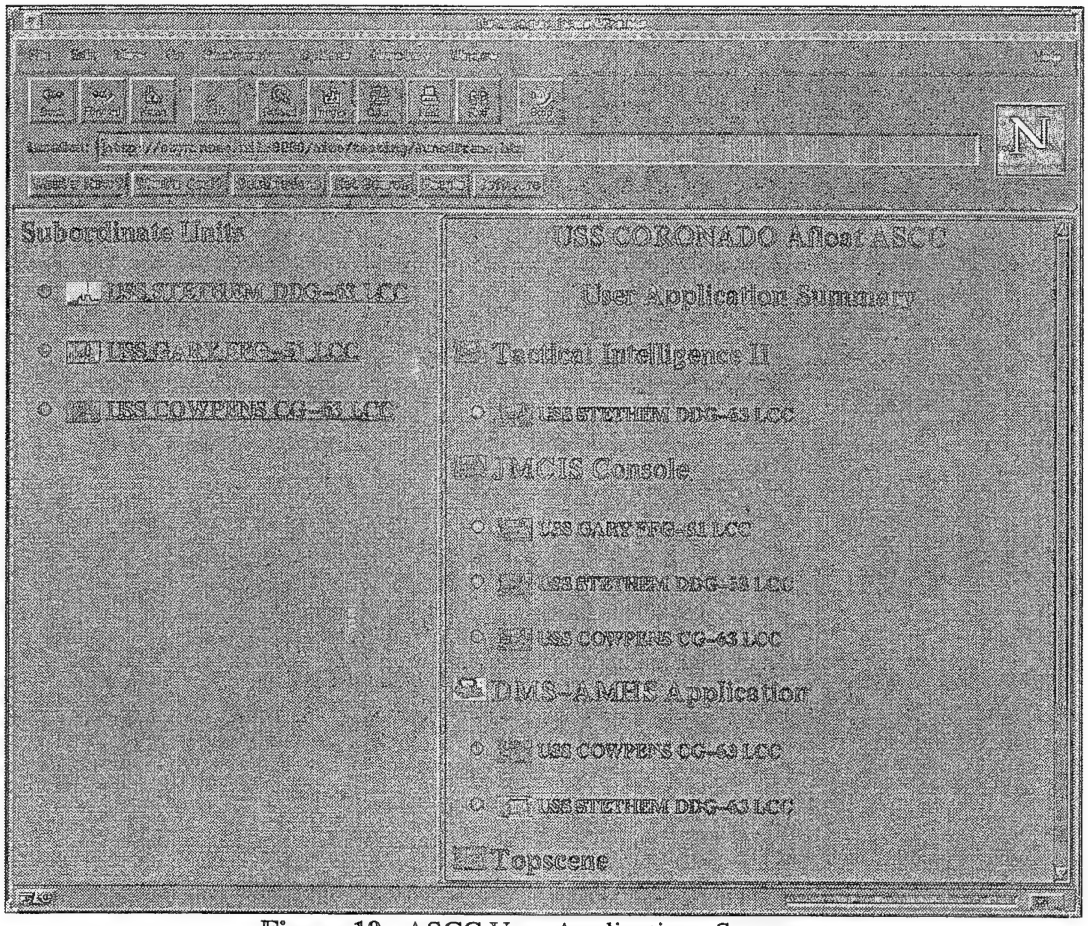


Figure 19. ASCC User Applications Summary

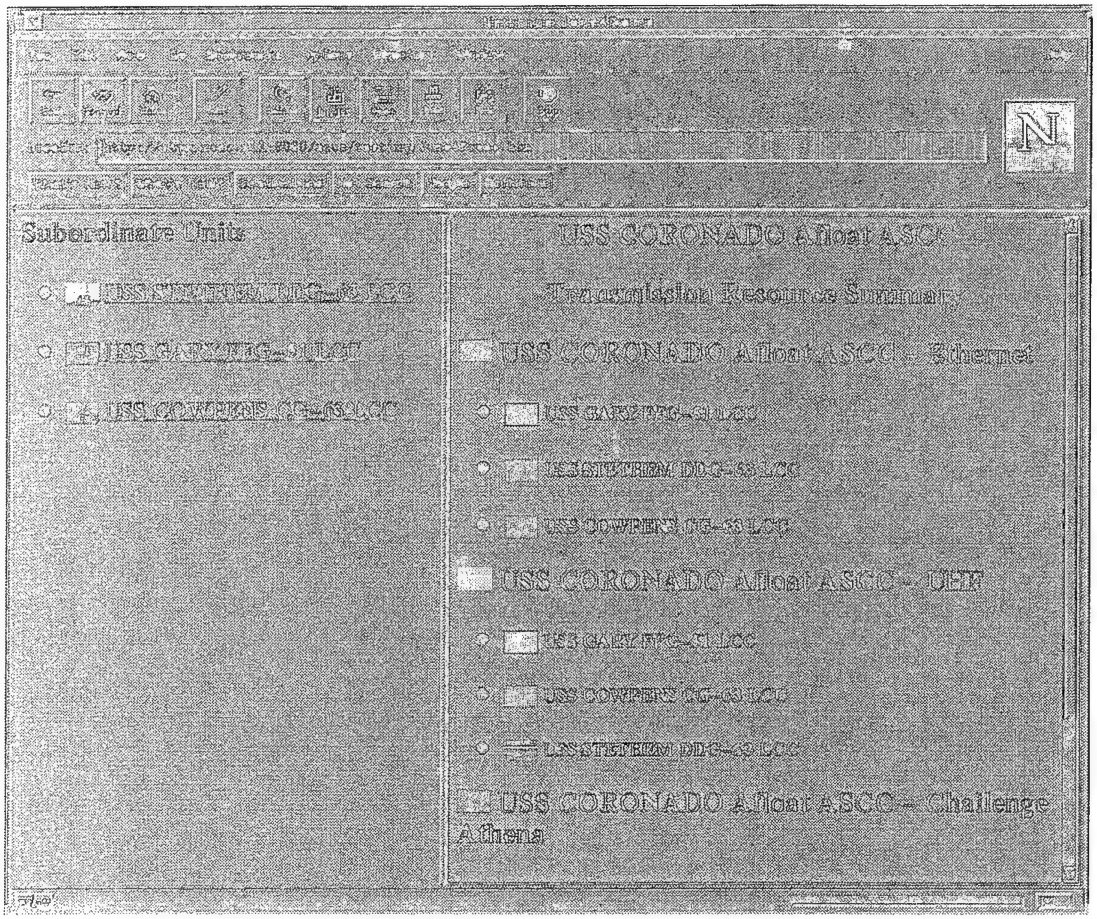


Figure 20. ASCC Transmission Resources Summary

3. Interface for the Naval Operations Center (NOC)

The interface for the NOC has not been developed yet. However, the concept is similar to the ASCC except on even a higher level. A NOC would normally be found ashore or on a major command and control ship such as the USS CORONADO AGF-11. The view at a NOC would have a number of ASCCs and maybe some individual LCCs. The managers and decision-makers at a NOC would be interested only in high level status information such as overall mission status and mission function areas.

D. WEB MASTER

To build Web pages and to keep a Web site up to date requires a Web master. Contractors can initially install the first sites for individual LCCs, ASCCs, and NOCs. However, it will take personnel assigned to those units to keep the sites current. Building Web sites is currently not required training. However, this talent is becoming easier with such vendor products as Microsoft Front Page and Hot Dog. Although the prototype did not show fancy graphics or multimedia capabilities, these certainly can be added in future upgrades.

VI. THE COMMUNICATIONS PLAN (COMMPLAN)

Since, the prototype is based on mission-centric network information, a tool is required to define and give the boundaries of a mission. That tool will be the Navy's Communications Plan (COMMPLAN). The COMMPLAN is typically a Navy paper-based message to units which outlines communications requirements. It can designate such parameters as what frequencies are to be used for different radio links. This is traditionally handled manually by technicians. A new direction will be given to the COMMPLAN as it applies to ADNS. It will be a software application that will be transmitted via available media to Local Control Centers (LCCs), Autonomous System Control Centers (ASCCs), and Network Operations Centers (NOCs) and automatically (no human intervention) manage certain aspects of the ADNS installation. For example, an ASCC or NOC can use the COMMPLAN to remotely reconfigure different resource requirements of subordinate LCCs. The COMMPLAN gives the essential parameters and definitions for ADNS. Thus if mission requirements change, a new COMMPLAN is issued. Such parameters can include (Casey, 1997): reallocating bandwidth, changing routing metric values to impact on how ships share communication resources, changing user priorities to reflect mission need, etc.

The COMMPLAN provides an excellent tool for remote network management. At the LCC level, management expertise will vary widely. Relatively junior personnel will be expected to be the network managers. The COMMPLAN allows higher authorities at the ASCC and NOC level to communicate requirements to LCCs with little involvement from the technical controllers. The COMMPLAN can also apply to the ASCC and NOC level with different level requirements. One of the biggest attractions of

the COMMPLAN is that its requirements will be automatically incorporated into the Network Management System. This allows a certain amount of transparency to the network managers at the local level. Figure 21 depicts the various functions that the COMMPLAN will have on different Autonomous Systems (AS).

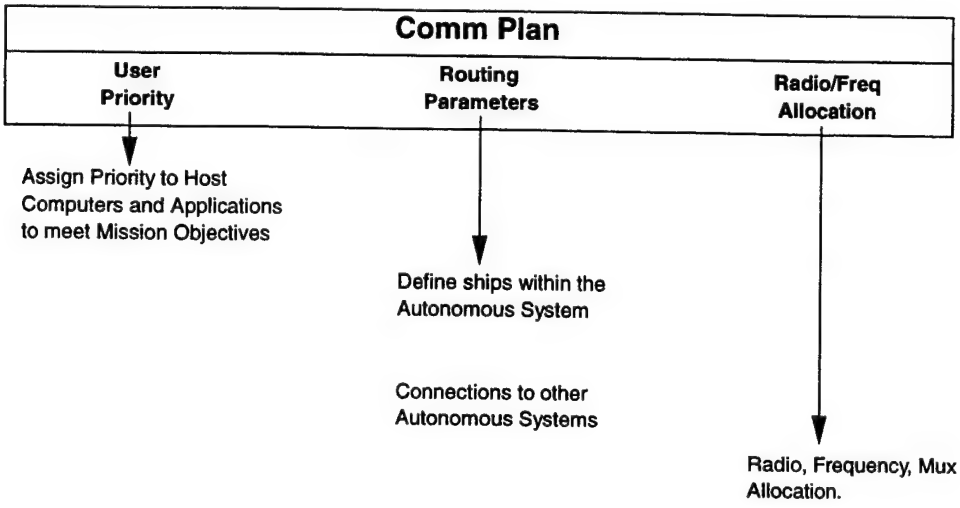


Figure 21. COMMPLAN Functions. After Ref [Casey].

A. INFORMATION FLOW UP THE HIERARCHY

For the COMMPLAN to be implemented from higher levels of management (ASCC or NOC), information flow is required from lower levels (LCC). For example if a ship (an LCC) joins an already formed Autonomous System such as another group of ships, the reporting hierarchy will have to be changed at the local level for the LCC. The use of the prototype described in Chapter V is an excellent platform to present status information to higher level managers. Managers at the NOC or ASCC level can then use that information to develop necessary requirements in the COMMPLAN for subordinates.

Although the sample Web pages in the prototype just show status information, it is possible that future Web pages can include additional information needed for the COMMPLAN such as bandwidth allocations and priority settings.

B. INFORMATION FLOW DOWN TO SUBORDINATES

As explained previously, the biggest attraction of the COMMPLAN is that is provides a means for remote network management. For example, a carrier battle group has a group of ships that can operate together as a Wide Area Network. Each ship conducts different tasks and missions. Suppose the missions for the group of ships now change and some ships have to disperse from the battle group to conduct other missions. This brings about a change in the boundary of the Autonomous System. The network manager on the carrier (an ASCC) now has to change such things as resource requirements, priority assignments, and routing parameters. To do this, COMMPLANs can be transmitted to all ships affected and the new network requirements can be configured automatically and remotely from the carrier. Take this scenario and extend it to the NOC on shore. It's conceivable that one NOC on shore can reconfigure the network requirements of many ASCCs and LCCs through the use of the COMMPLAN. Table II shows different affects that the COMMPLAN has on the LCC, ASCC, and NOC.

LCC	Orders Down	Reconfigure Router Priorities, Queue Thresholds, IP Addressing Plans
	Report Up	Reconfigure Status of Reports to ASCC or NOC
ASCC	Orders Down	Reconfigure LCC Priorities and Resources in ASCC when mission changes
	Report Up	Reconfigure Status of Reports to NOC
NOC	Orders Down	Reconfigure LCC and ASCC Priorities and Resources
		Redefine ASCC and LCC relationships in a given Autonomous System

Table II. Examples of COMMPLAN Implementations on Different AS Levels

Figure 22 shows the flow of direction of the COMMPLAN from the ASCC or NOC to lower levels.

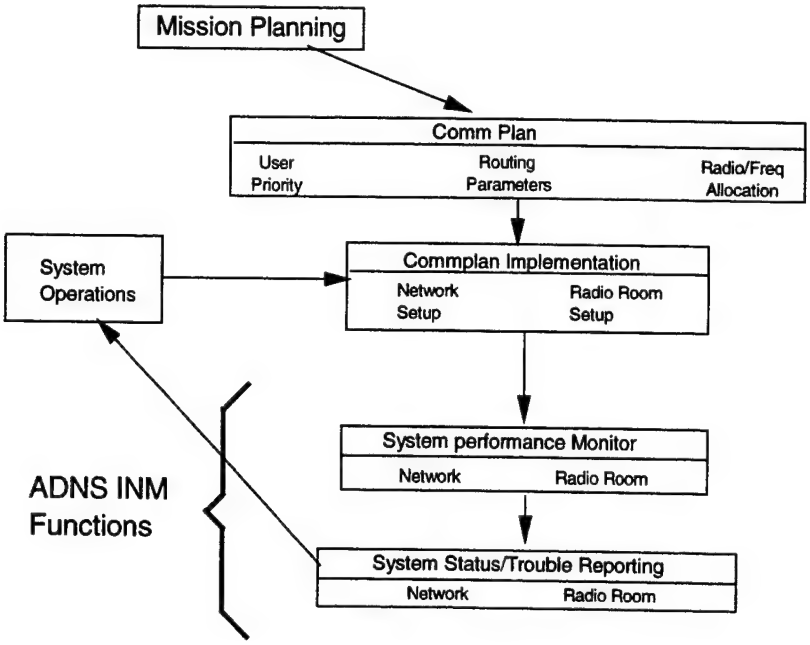


Figure 22. COMMPLAN Flow Down. After Ref [Casey].

Thus the COMMPLAN will have different effects, depending on the level of management. First the mission needs to be defined. Then other requirements are defined such as: define user priorities to accomplish the mission, define the AS's, and define the resources between AS's. The COMMPLAN is mainly used as a means for automatic one way configuration and management from the NOC or ASCC which provides a powerful tool for combat effectiveness (Casey, 1997).

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

If the Navy is about to get under way with a new process of doing business, it needs to re-evaluate its current traditions and cultures of internal, centralized micro-management. It is clear that ADNS is one major tool to bring about this change towards a network-centric way of conducting business. However because of the unique roles of the Navy, it is crucial to adapt the network to support the mission and not the other way around.

Using mission-centric network management tools to manage networks are a step in this direction. Using a Web based interface to accomplish these goals allows managers on all levels to view and manage information from any desktop. Network management concepts can be very complex and detailed, and many managers and decision-makers do not need the detailed information that many commercial products offer. What is desired instead, is to know how the network affects Navy tasks and missions. Using the Web brings these powerful capabilities and is easy to use. With more and more enhancements being added to the Web, the future holds many possibilities on how the Navy will take advantage of using the Web for carrying out its mission-centric network management needs.

B. RECOMMENDATIONS

The following recommendations address the topics discussed in Chapter VI. Although this thesis has been focused on a Web-based network management tool, there are many areas to improve the Navy's goal of network management.

- **Web-based Mission-centric Network Management Tools**: The prototype in this thesis is an initial attempt to present mission-centric network management information and is more conceptual than implementation oriented. Further research is required to interview Navy users and to analyze and map exact requirements for future enhancements of any mission-centric Web pages. Also recommend using a Navy unit such as an aircraft carrier as a case study to document the exact architecture requirements for future Web pages.
- **Education and Training:** Proper education and training is required for all levels of network managers. On the job training can suffice for the near term. However, to instill the proper mindset to a network-centric approach, standardized training will have to be developed. For officers this can be obtained via P-code. For enlisted personnel this can be obtained via A-school or vendor specific training.
- **Webmaster:** If Web-based technology is eventually adopted, webmasters will be required at all levels: LCCs, ASCCs, and NOCs. Mission and unit specific information will have to be updated on a regular basis. This will require designating the proper personnel with proper training to keep Web-pages current. However, this skill becomes easier and friendlier with available commercial products.

The goal of this thesis is to clarify some concepts in network management and the Navy's approach to be network-centric. The prototype is just one view to look at applying mission-centric requirements on a Web-based interface. Future enhancements can include many of the Web's attractions such as graphic and multimedia extensions.

APPENDIX A. NETWORK MANAGEMENT ISSUES REQUIRING FURTHER CLARIFICATION AND RESEARCH

A. STEPPING OUT OF THE BOX

These issues are not directly related to the thesis of Web-based network management. However, these are important issues to highlight because of their relevance to the Navy's approach to network management. There is no doubt that adopting a network-centric approach of doing business will break institutionalized paradigms in the Navy. A Navy ship at sea will have to shed it's centralized culture and way of conducting business to be successful. Therefore, there are many challenges to the Navy culture. Traditionally for a worker to accomplish a task, there were many redundant supervisory steps taken to ensure the quality of work. However, this wasted many hours of work both for managers and workers, which in turn delayed other tasks.

Just like how corporate organizations learned to conduct business in a decentralized fashion, the Navy will have to shed it's grip on traditional culture and learn to empower and trust it's workers. In today's times of fiscal and political pressures, the Navy cannot afford the luxury of excess manpower and redundancy.

B. CHIEF INFORMATION OFFICER (CIO)

A position relatively new to the Navy is the CIO. Although plans have already been devised to set up CIOs in some Navy organizations such as aircraft carriers, the CIO concept will need to trickle down all the way to individual units. The CIO should be responsible for all the networks in the organization no matter what department the networks are located in. The CIO should also have the necessary staff with the requisite knowledge to manage the organization's networks. Currently the Navy billets almost

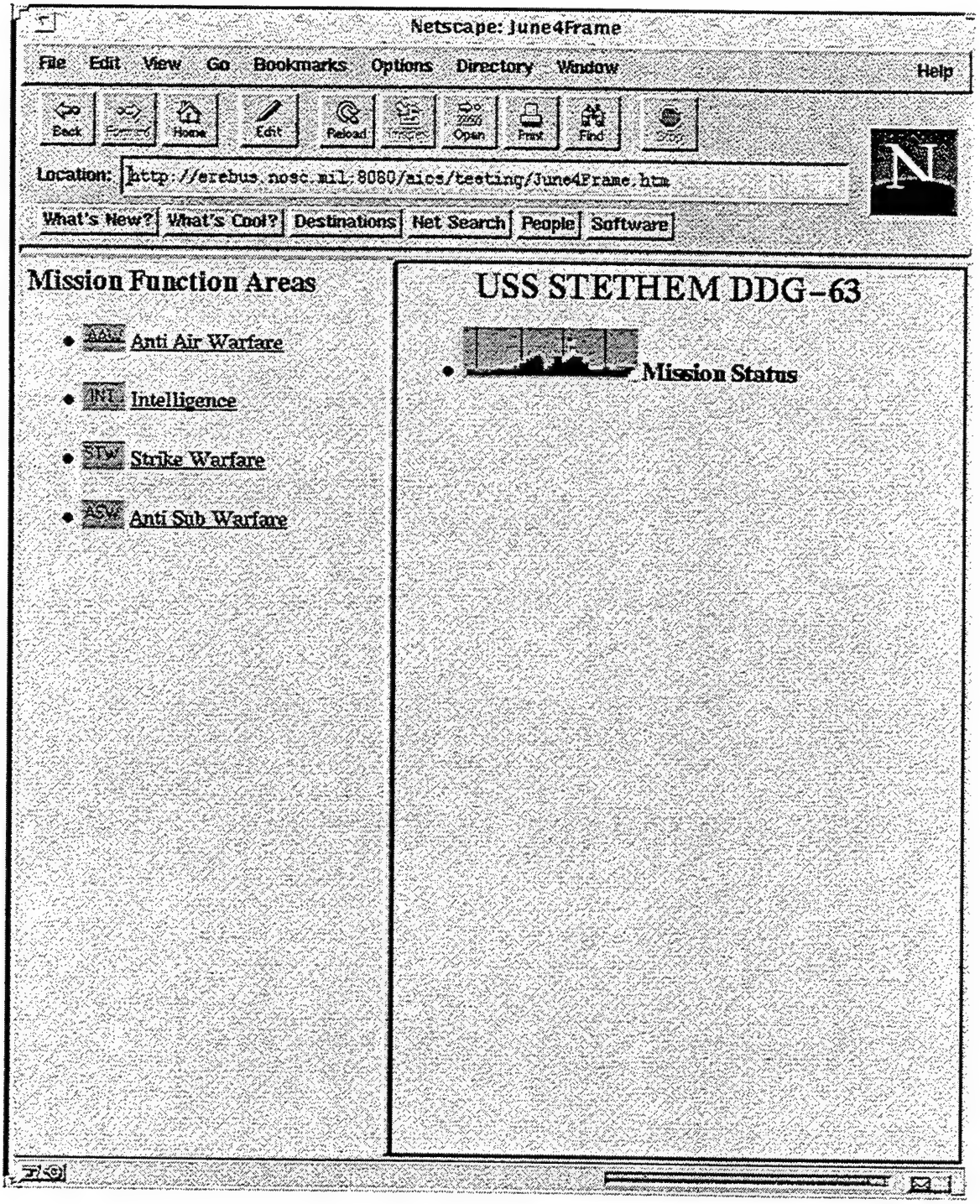
every unit with a communications officer who is normally in charge of that unit's network. However, the communications officer is often a junior individual without the proper expertise in network management.

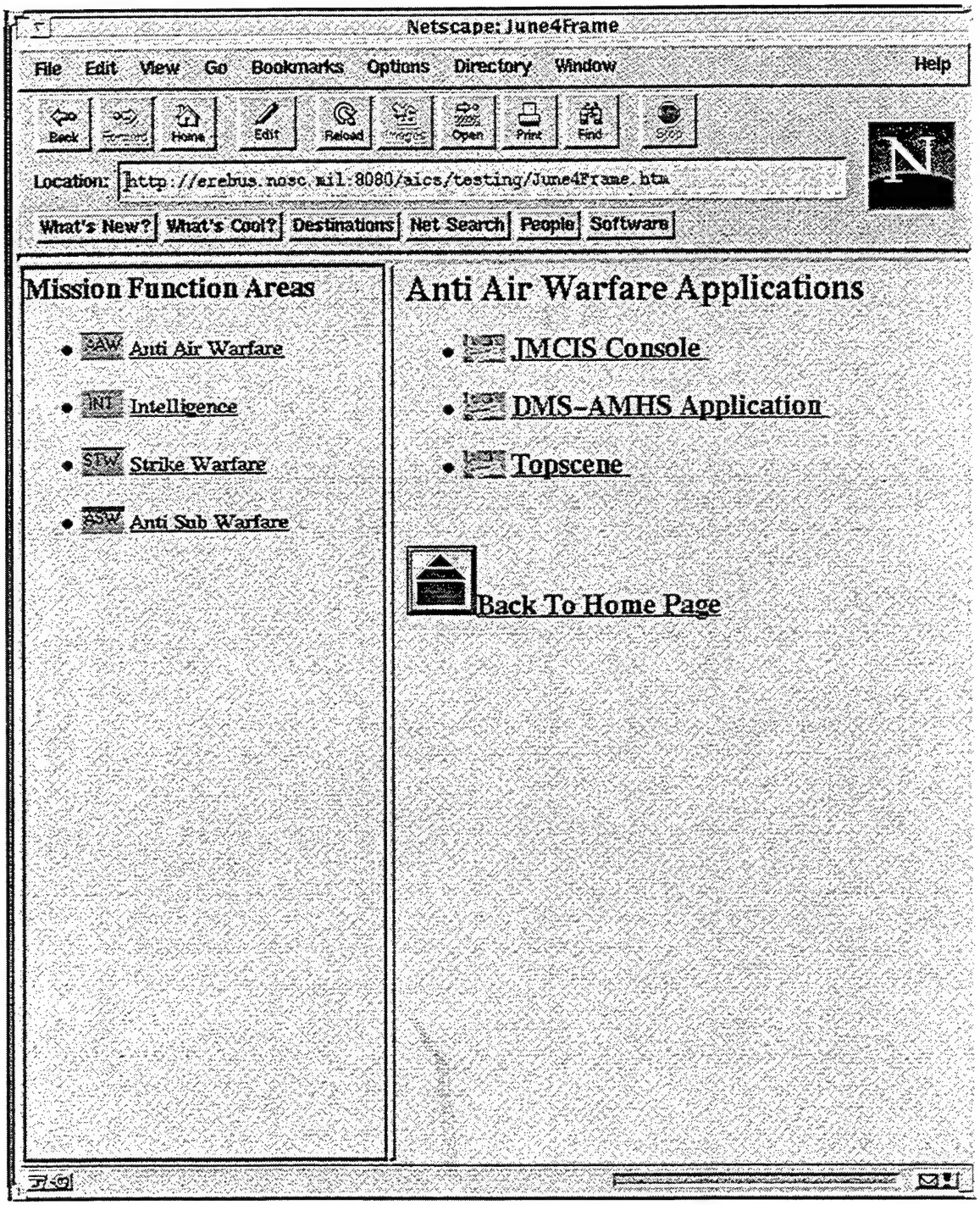
C. PROPER EDUCATION AND TRAINING

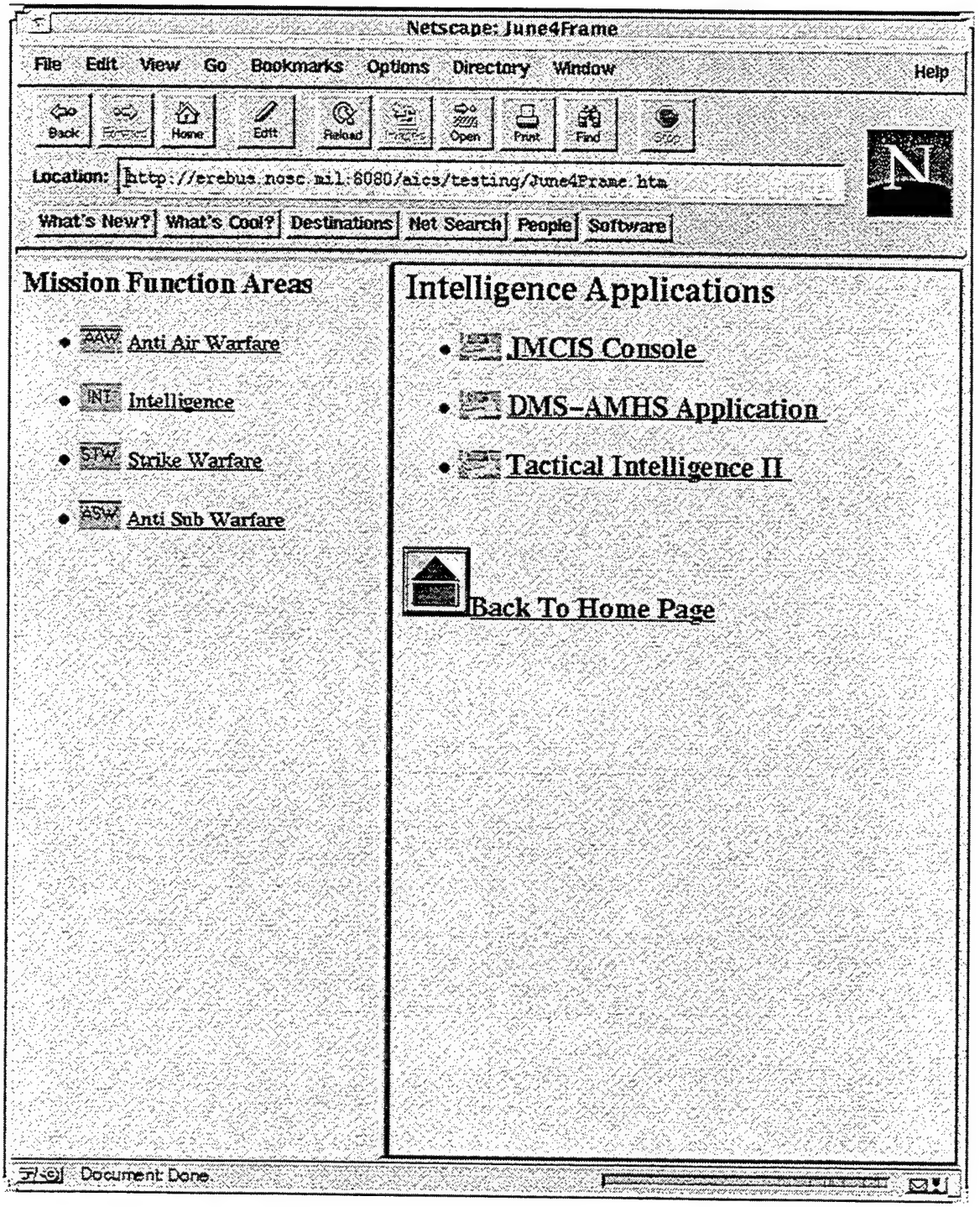
The requirement of necessary network management expertise for managers and technicians is easier stated than achieved. Navy technicians are educated shortly after boot camp and this training can take up to two years to complete. Currently there is no firm requirement to be a qualified CIO or network manager. Upon commissioning, Navy officers can go to a wide variety of jobs that often do not utilize the degree that the officer obtained. Officers can obtain a professional code (P-code) through a masters program that indicates a job sub-specialty such as in information technology management. A popular path to obtain a P-code is through the Naval Postgraduate School (NPS) where officers can work on a masters degree up to two years on full salary. However, because of strict promotion guidelines, the P-code is often disregarded for job assignments. Refresher education would also be required to keep up with technological changes. The point is, is that in the case of proper education and training for CIOs, it takes a lot of time and money to groom the right personnel. Since network technology changes rapidly, it also takes constant education to keep pace with the advances.

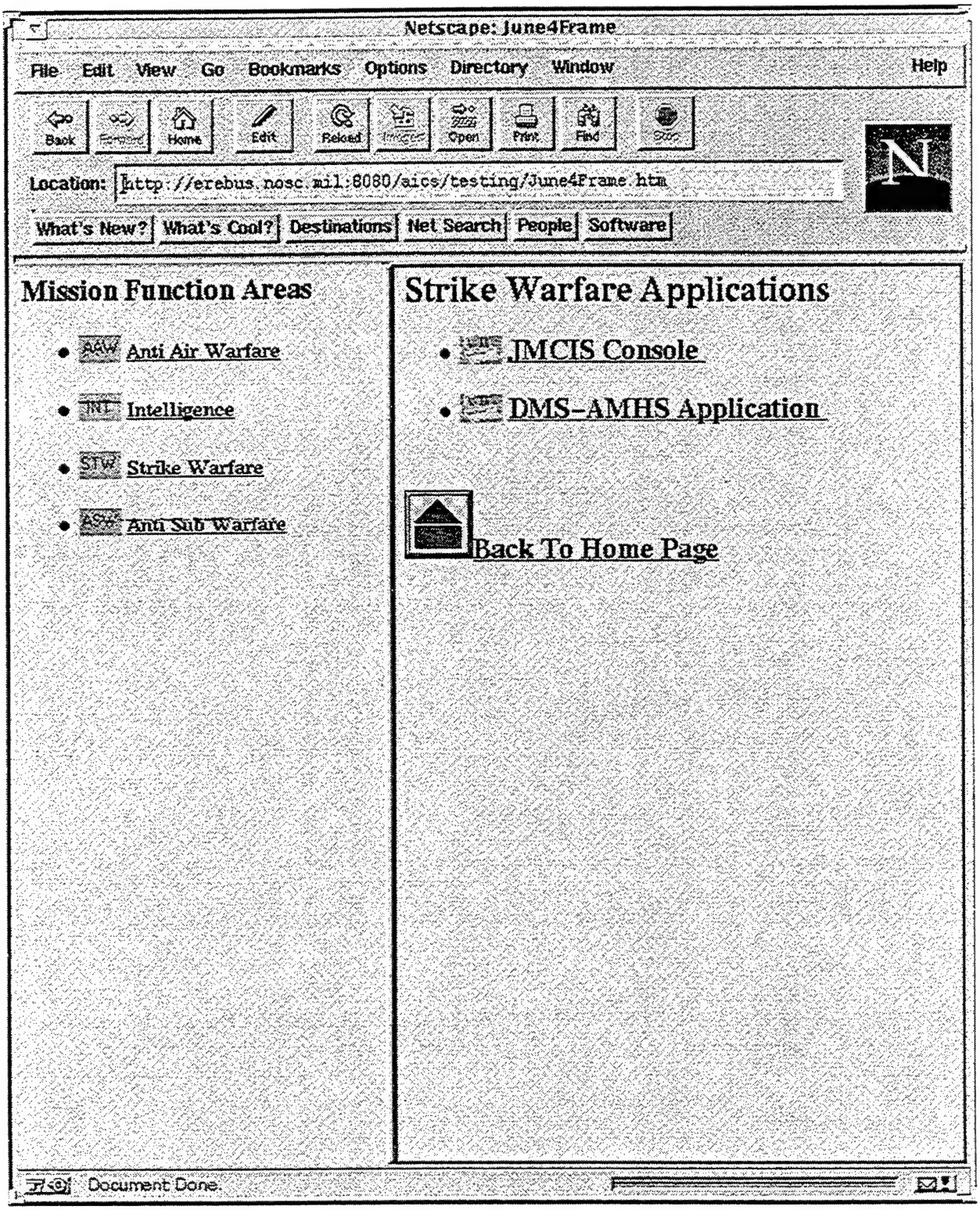
APPENDIX B. SAMPLE WEB PAGES FROM PROTOTYPE

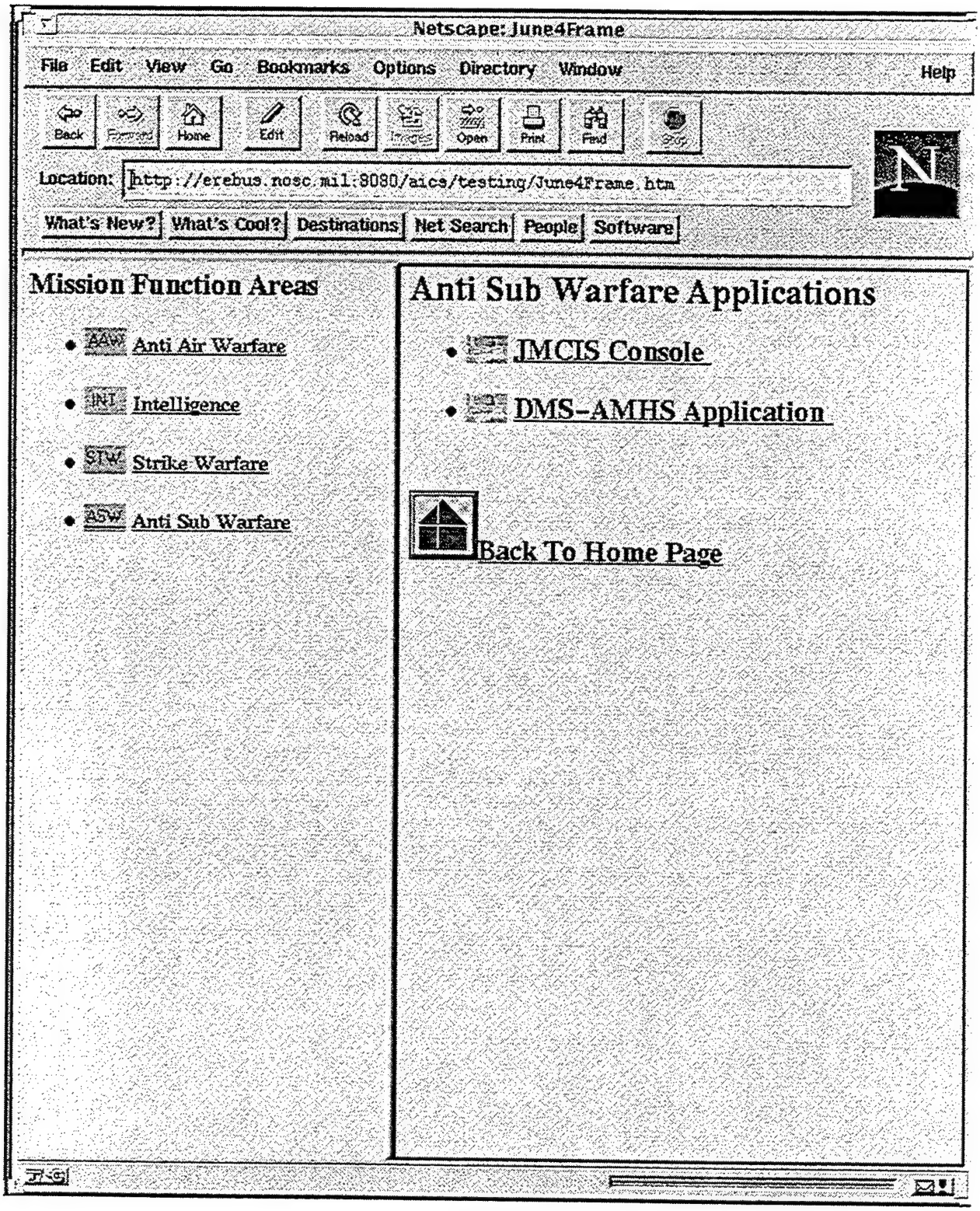
Appendix B is the collection of all the Web pages developed for the prototype in this thesis. The examples used do not represent the actual applications and information found on the ships listed. It is instead, an attempt to convey the idea and the potential to represent mission-centric network management information in a Web-based interface.

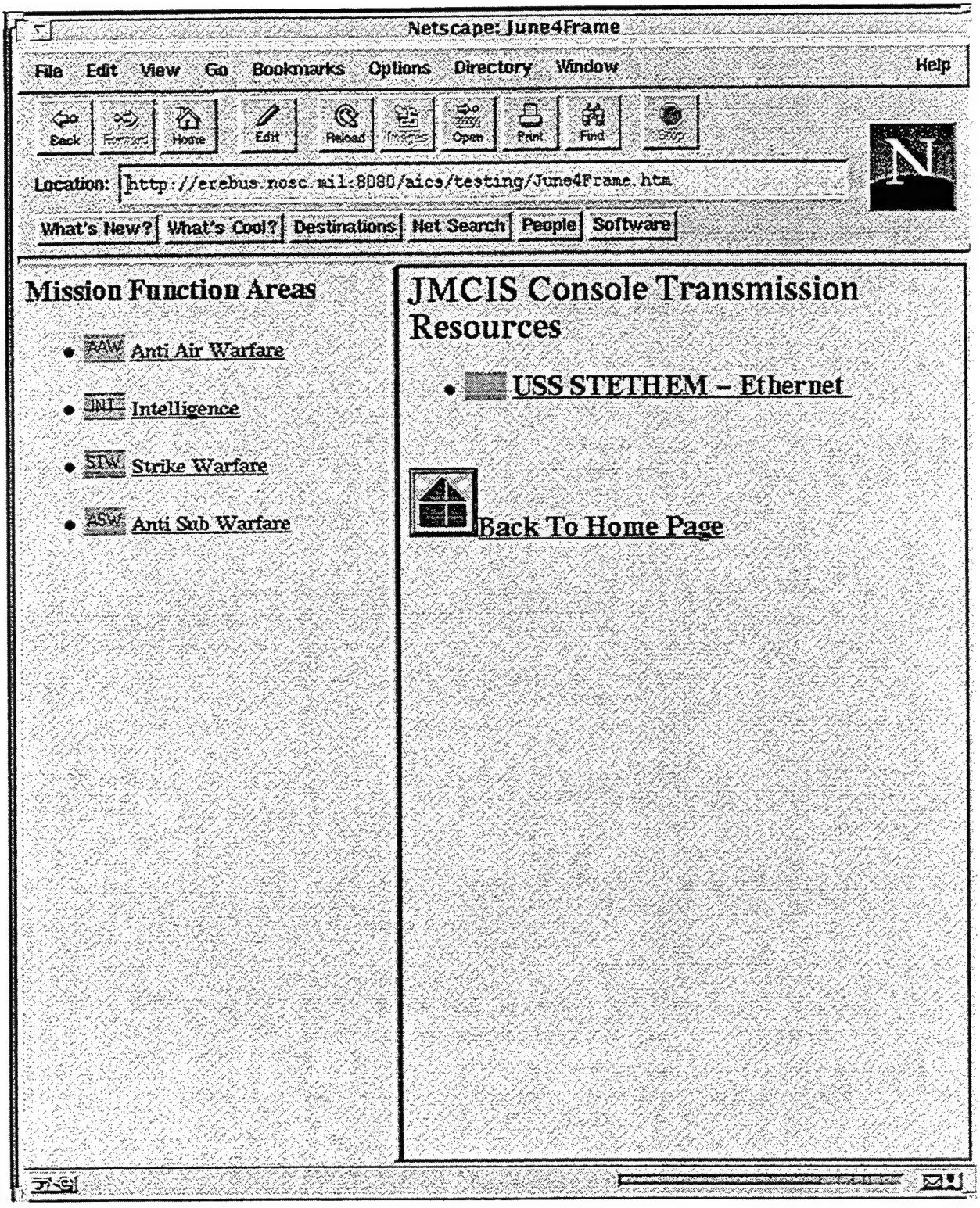

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
USS STETHEM DDG-63
Mission Status

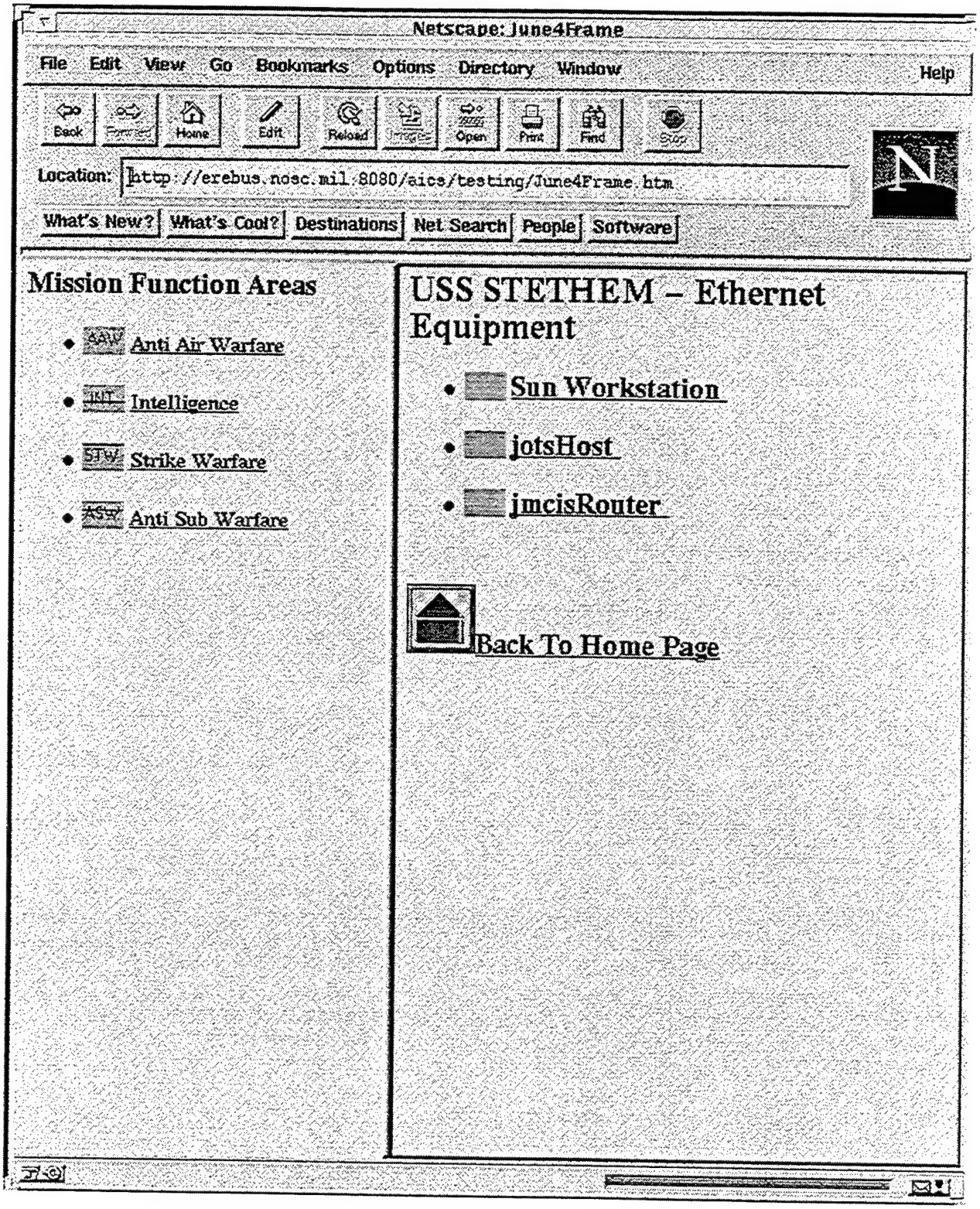

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
Anti Air Warfare Applications
JMCIS Console
DMS-AMHS Application
Topscene
Back To Home Page

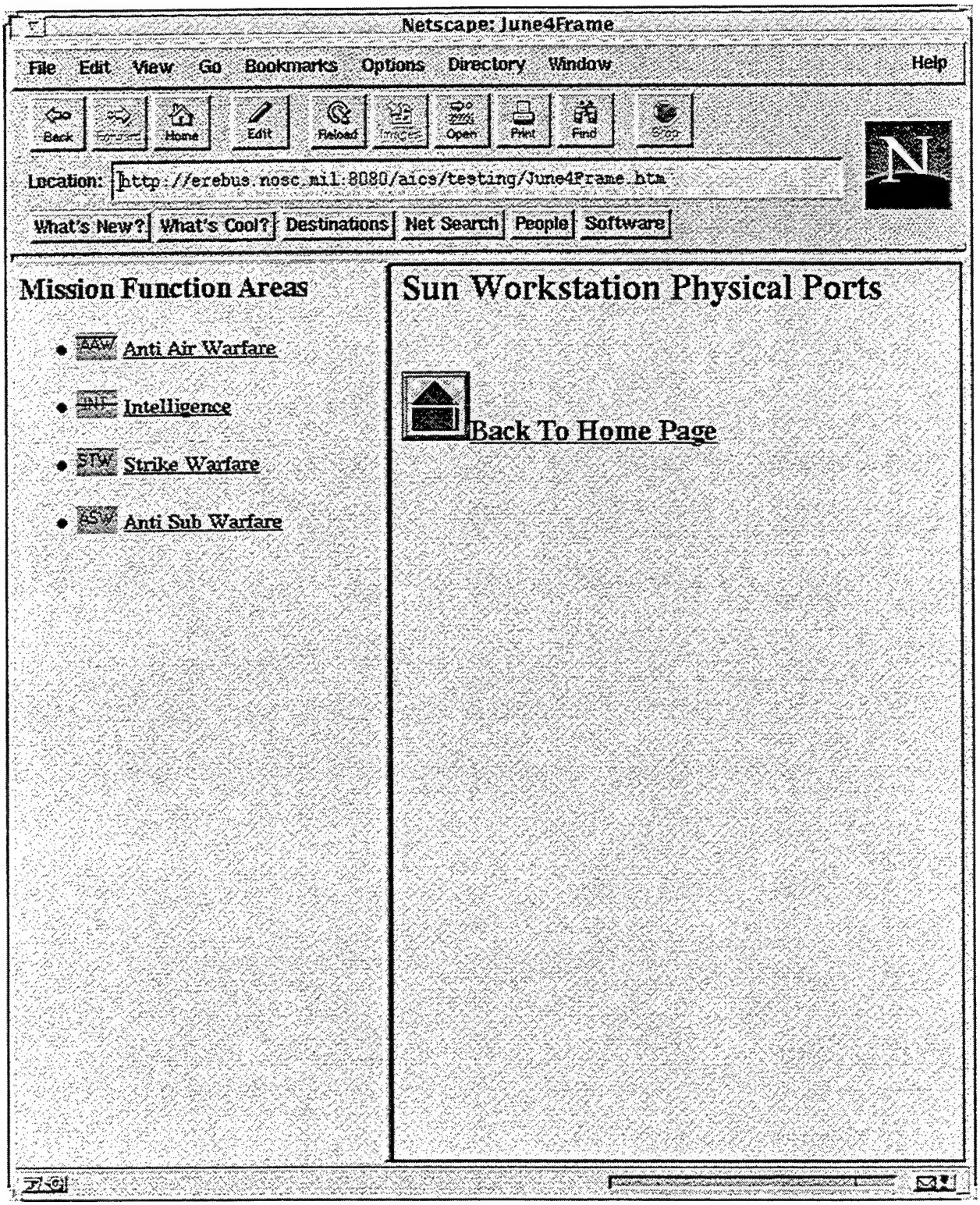

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
Intelligence Applications
IMCIS Console
DMS-AMHS Application
Tactical Intelligence II
Back To Home Page
Document Done

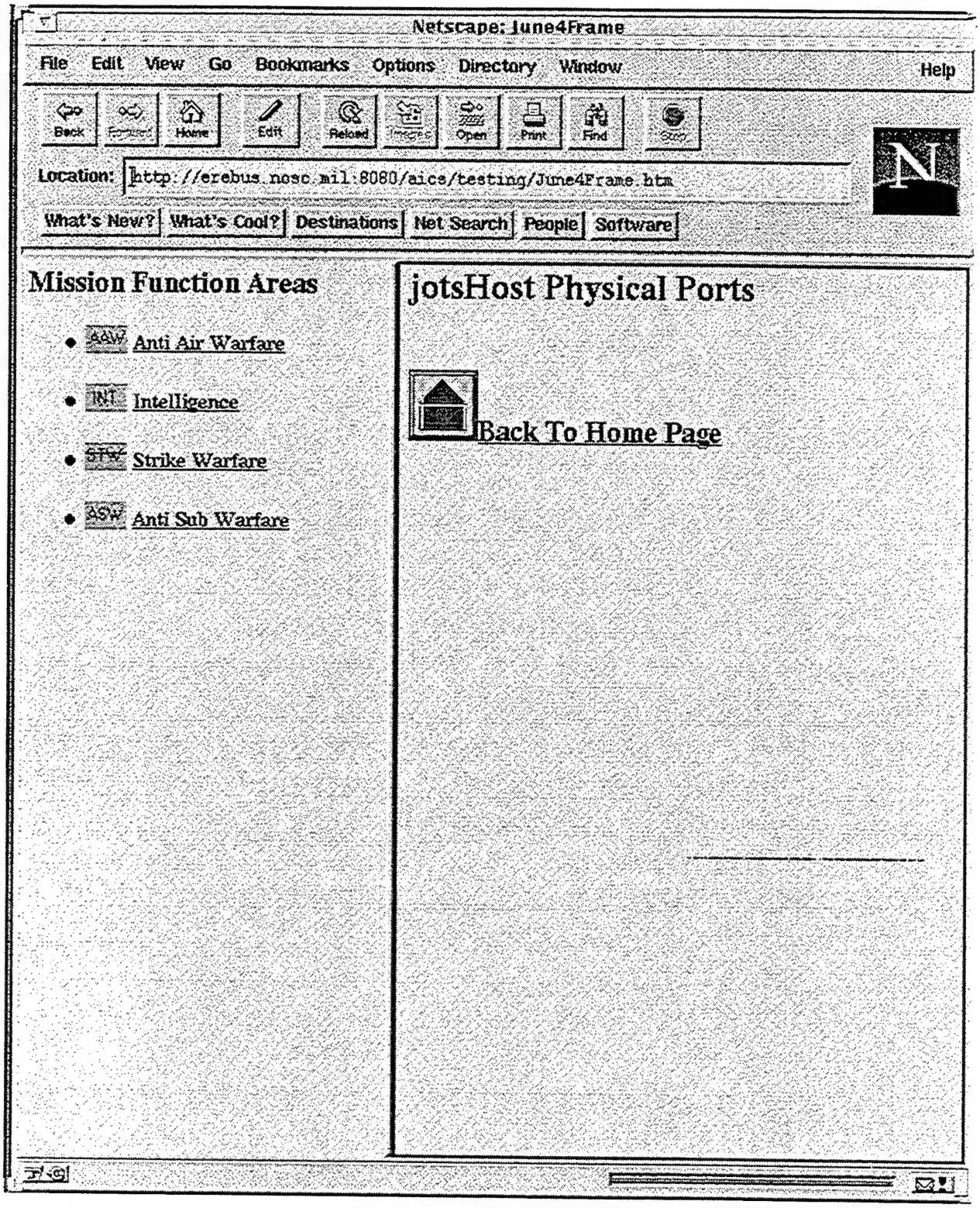

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
Strike Warfare Applications
JMCIS Console
DMS-AMHS Application
Back To Home Page
Document Done.

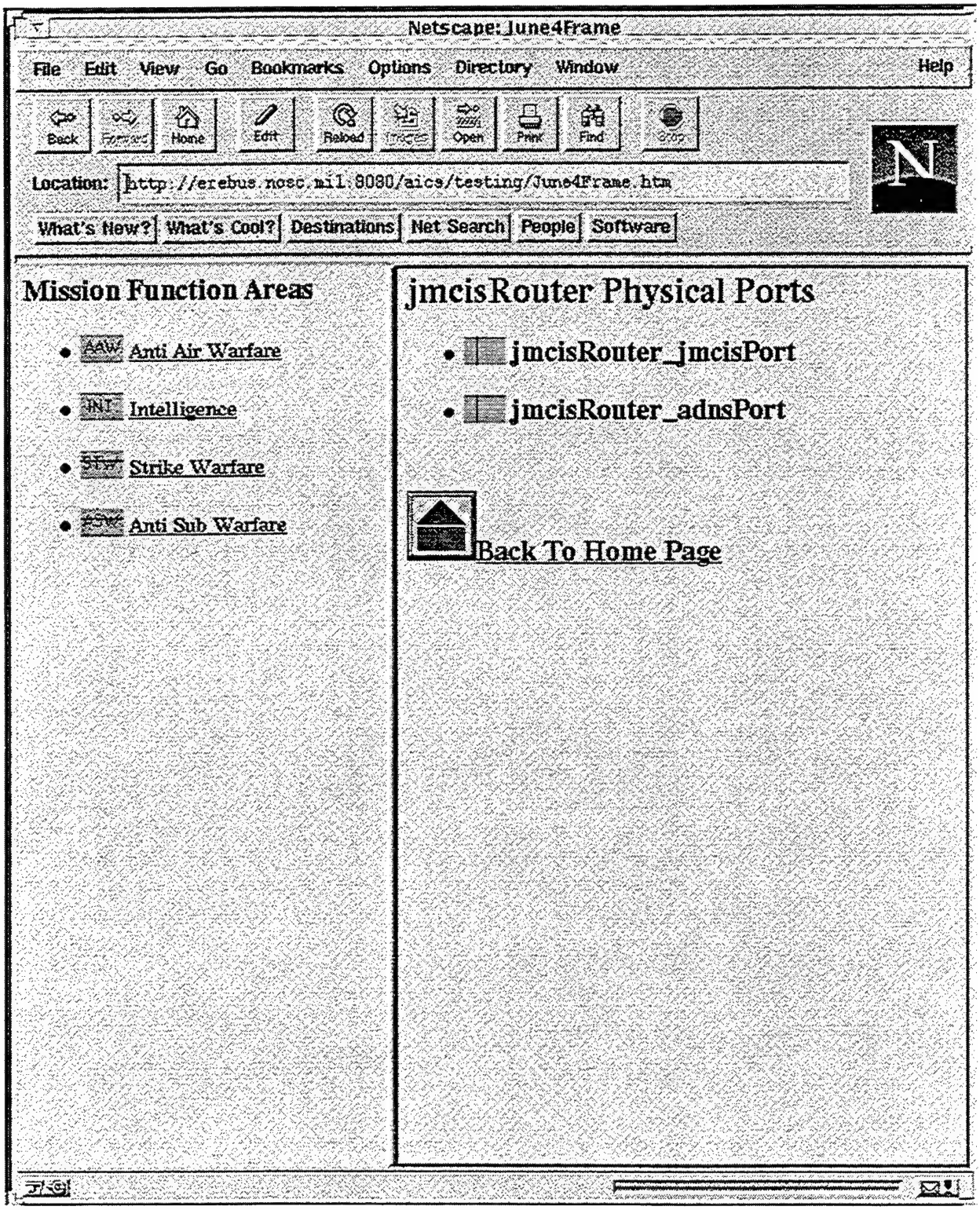

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aice/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
Anti Sub Warfare Applications
JMCIS Console
DMS-AMHS Application
Back To Home Page

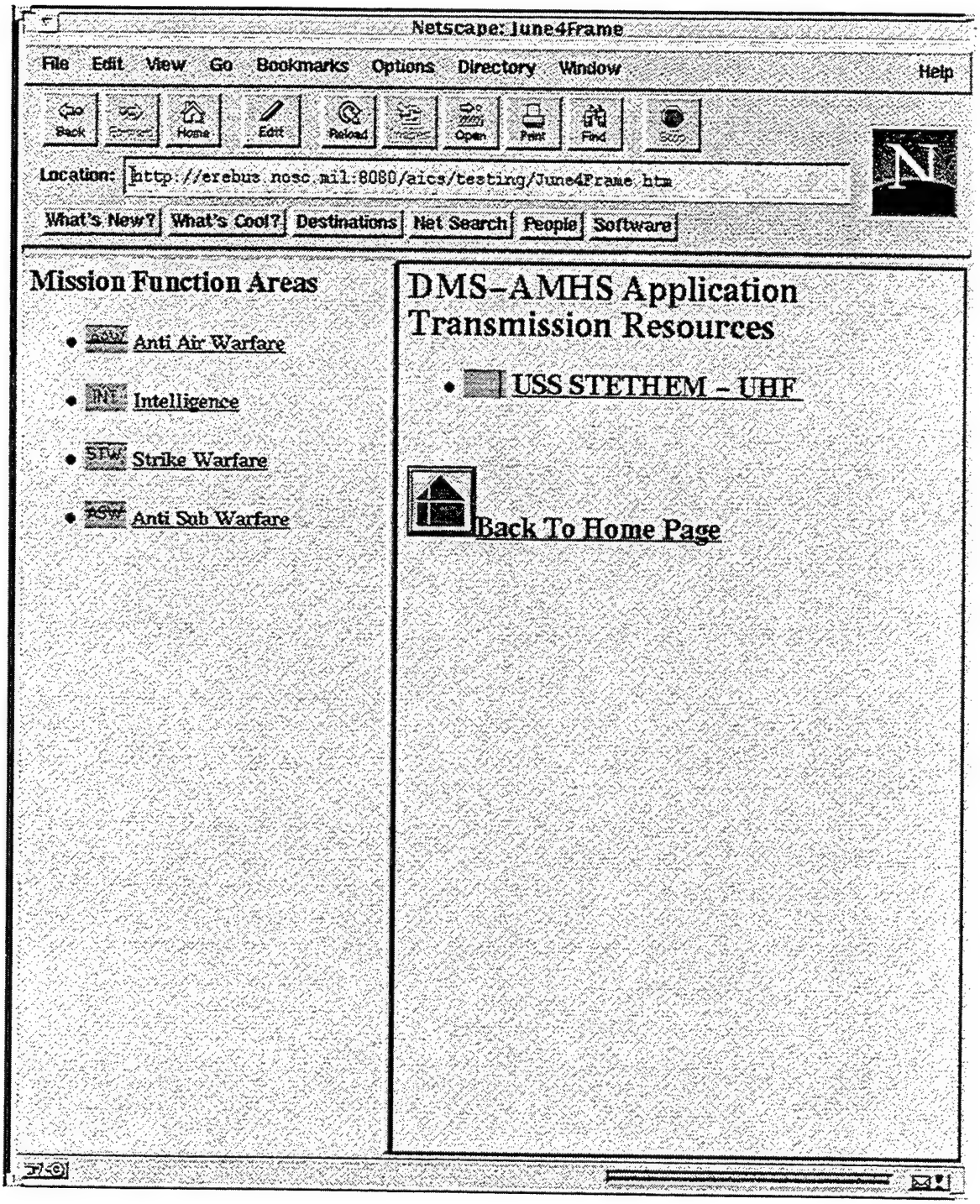

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
JMCIS Console Transmission Resources
USS STETHEM – Ethernet
Back To Home Page

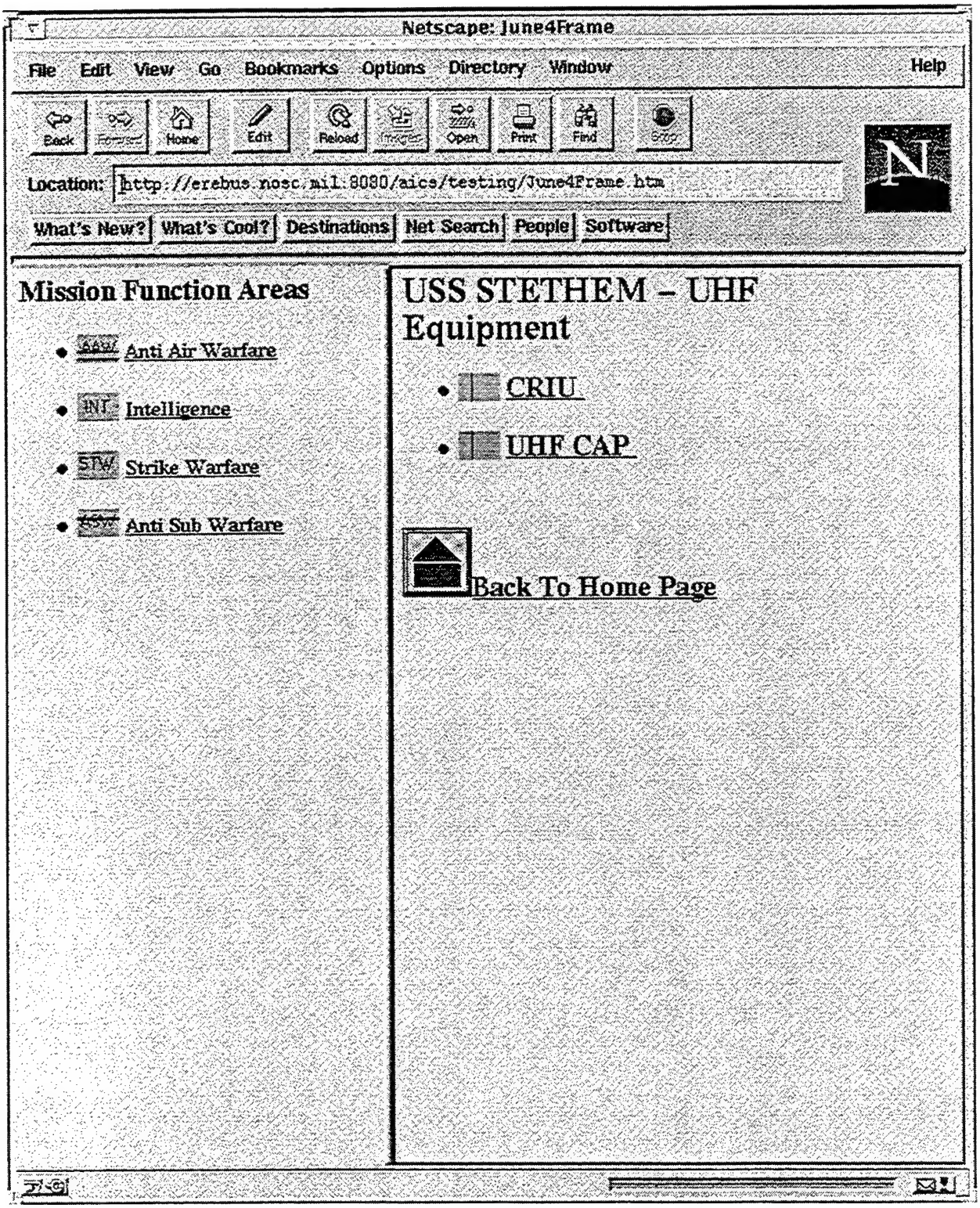

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
USS STETHEM – Ethernet Equipment
Sun Workstation
jotsHost
jmcisRouter
Back To Home Page

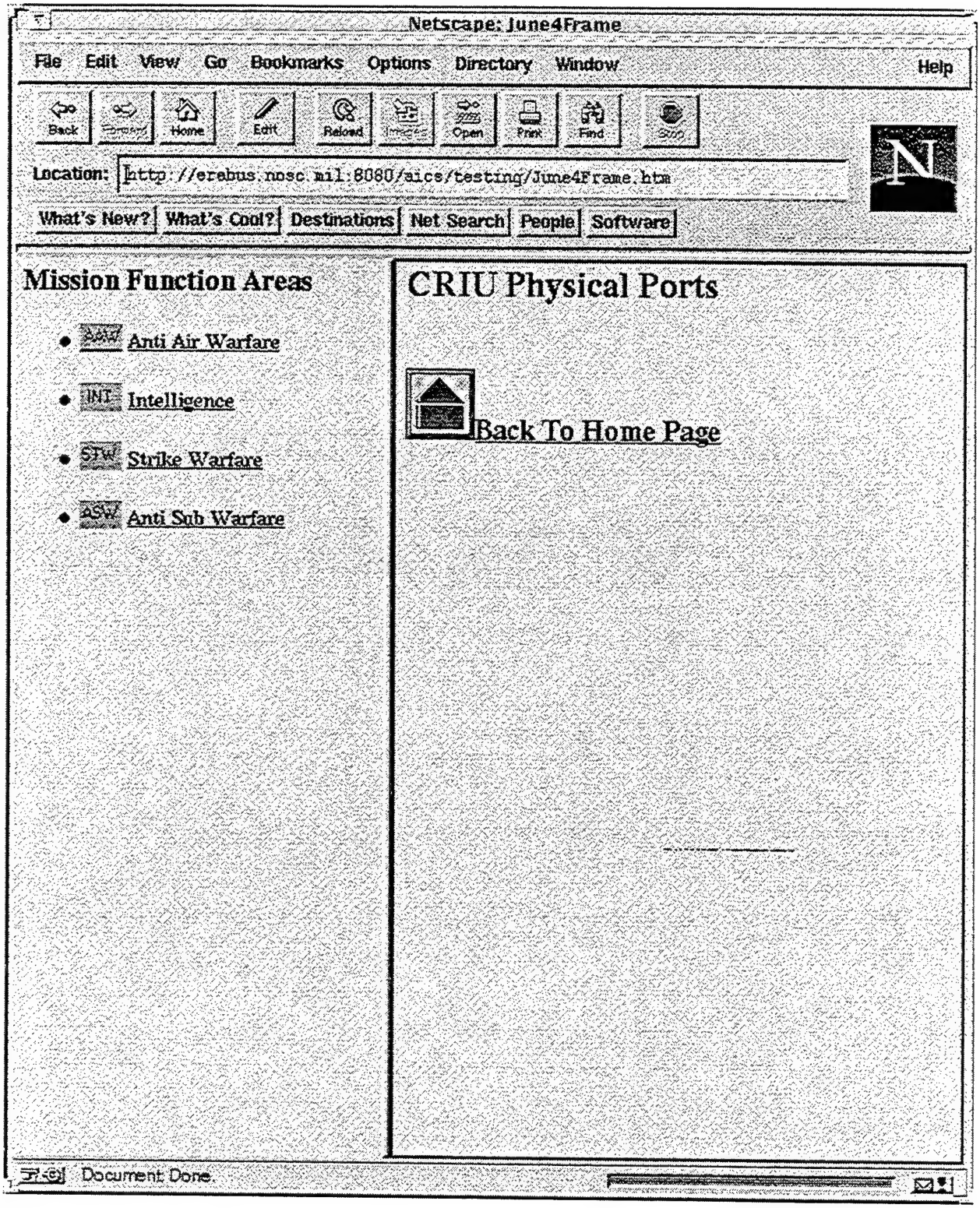

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
Sun Workstation Physical Ports
Back To Home Page

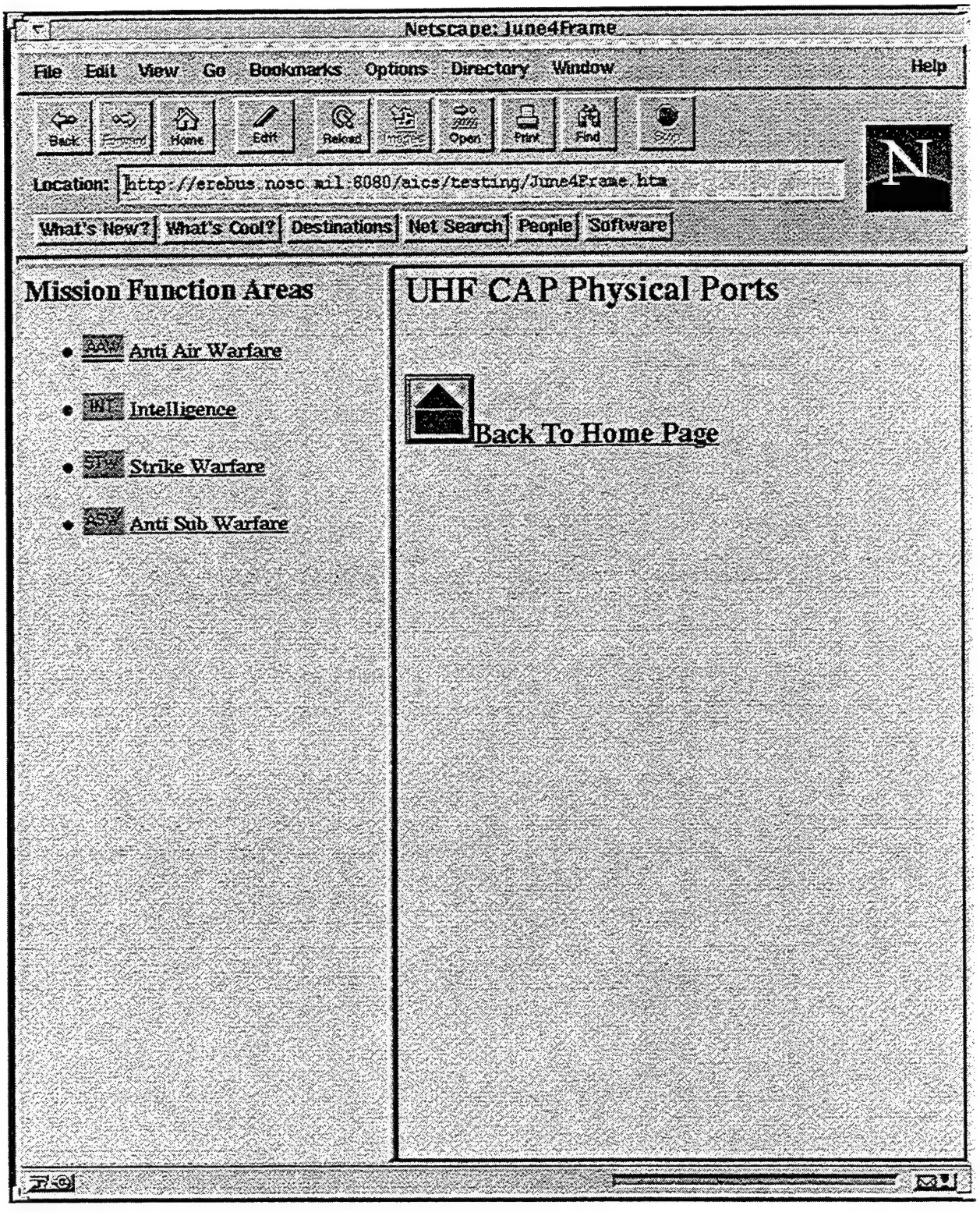

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
jotsHost Physical Ports
Back To Home Page

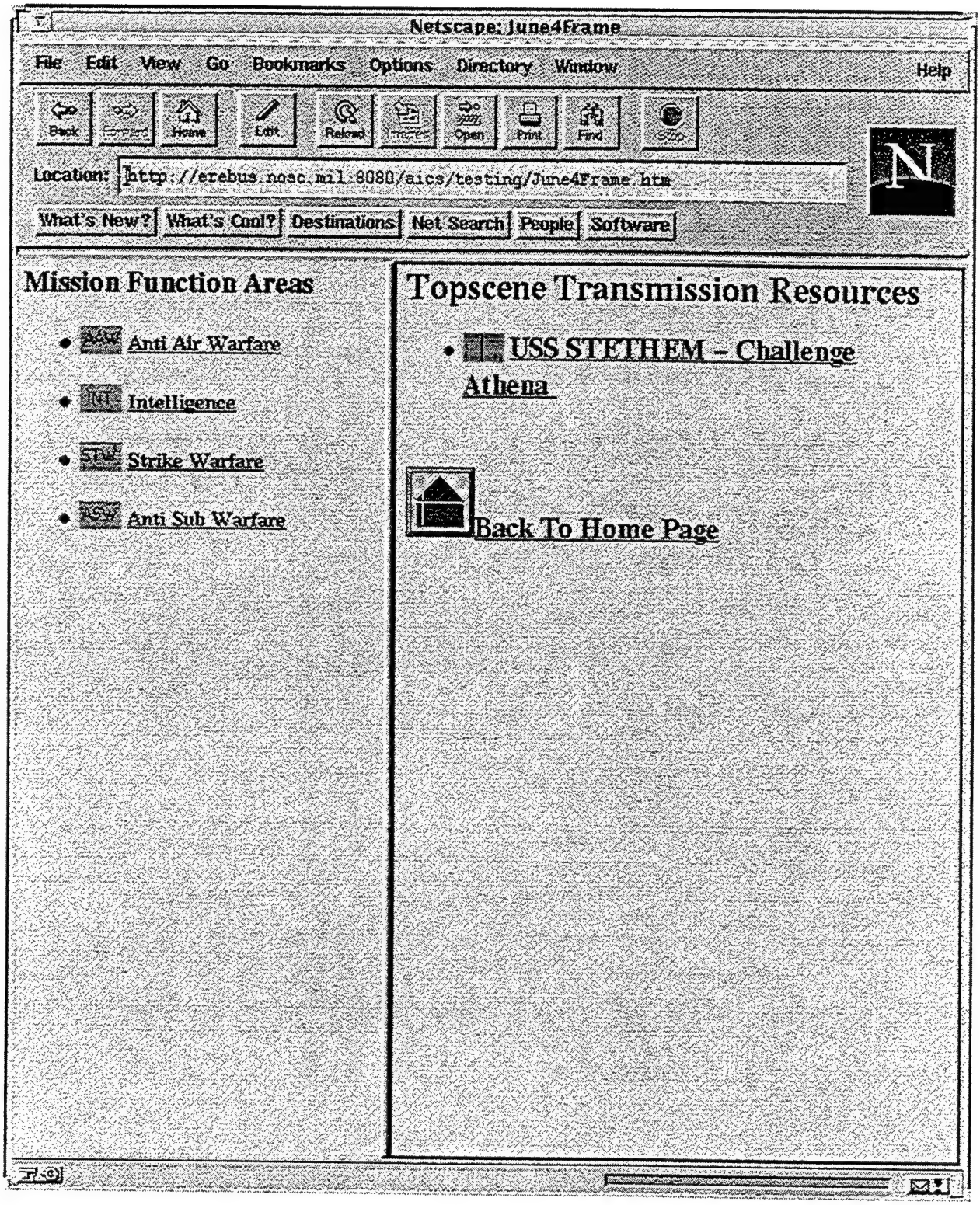

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
Strike Warfare
ASW Anti Sub Warfare
jmcisRouter Physical Ports
jmcisRouter_jmcisPort
jmcisRouter_adnsPort
Back To Home Page

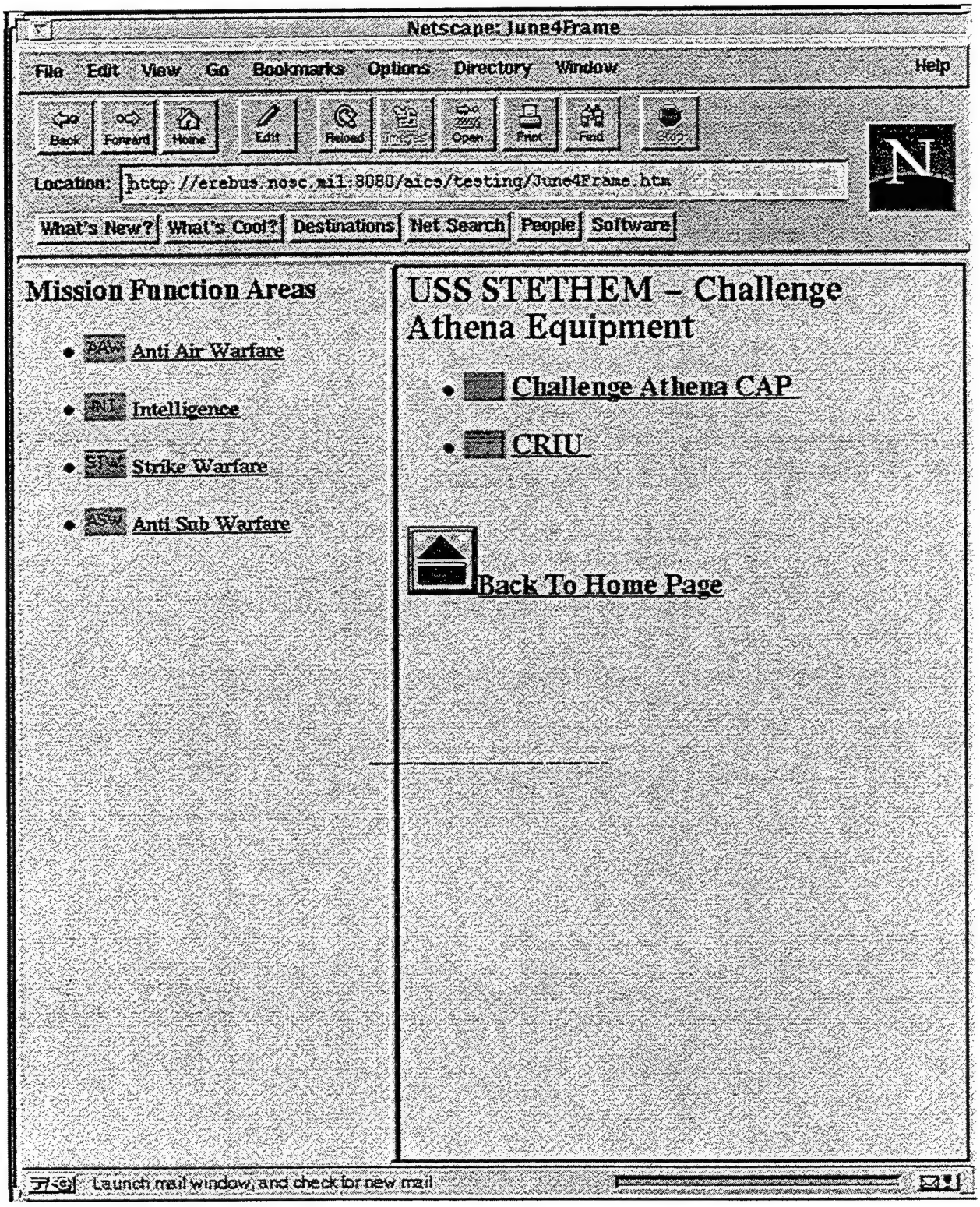

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
DMS-AMHS Application Transmission Resources
USS STETHEM - UHF
Back To Home Page

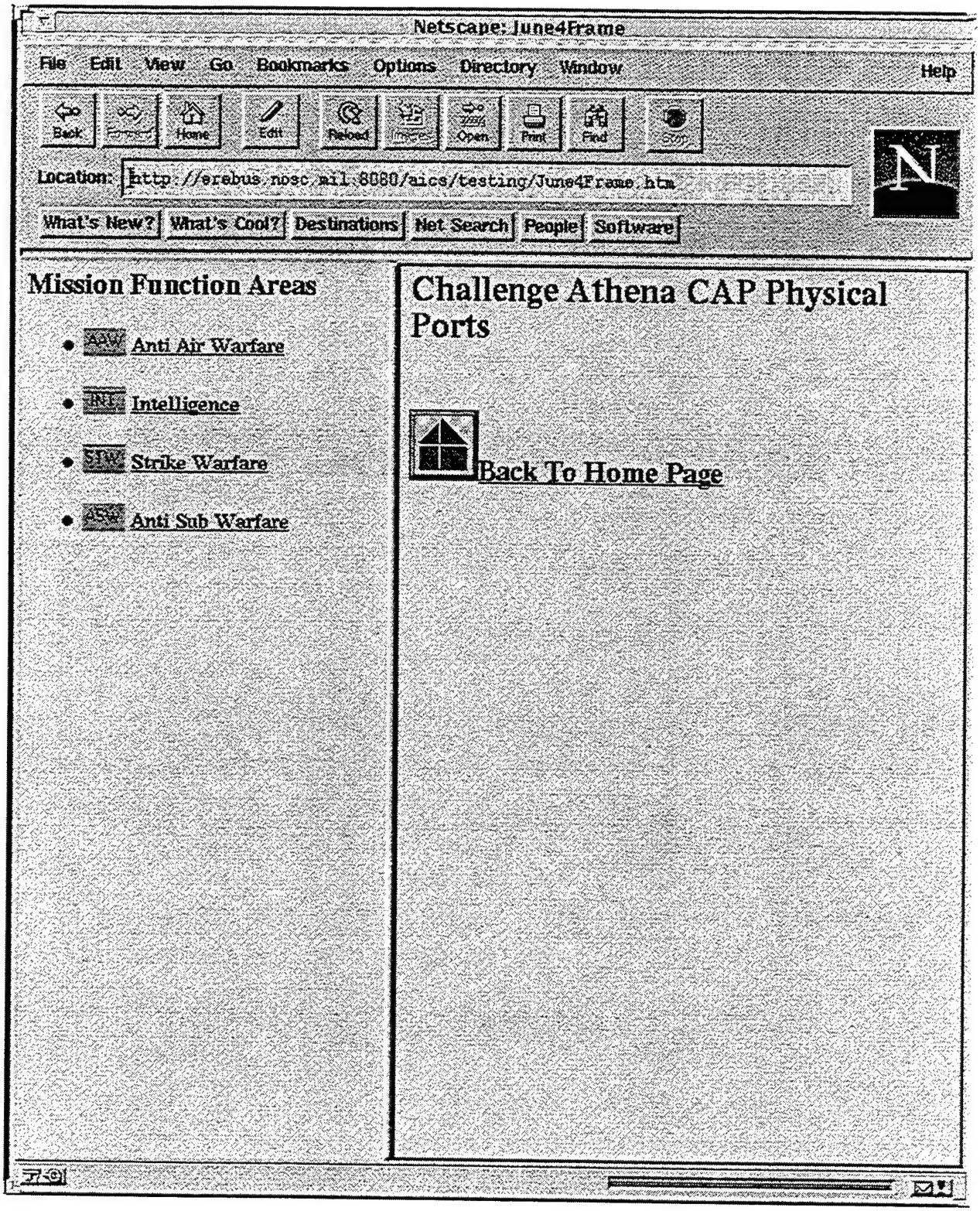

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
USS STETHEM – UHF Equipment
CRIU
UHF CAP
Back To Home Page

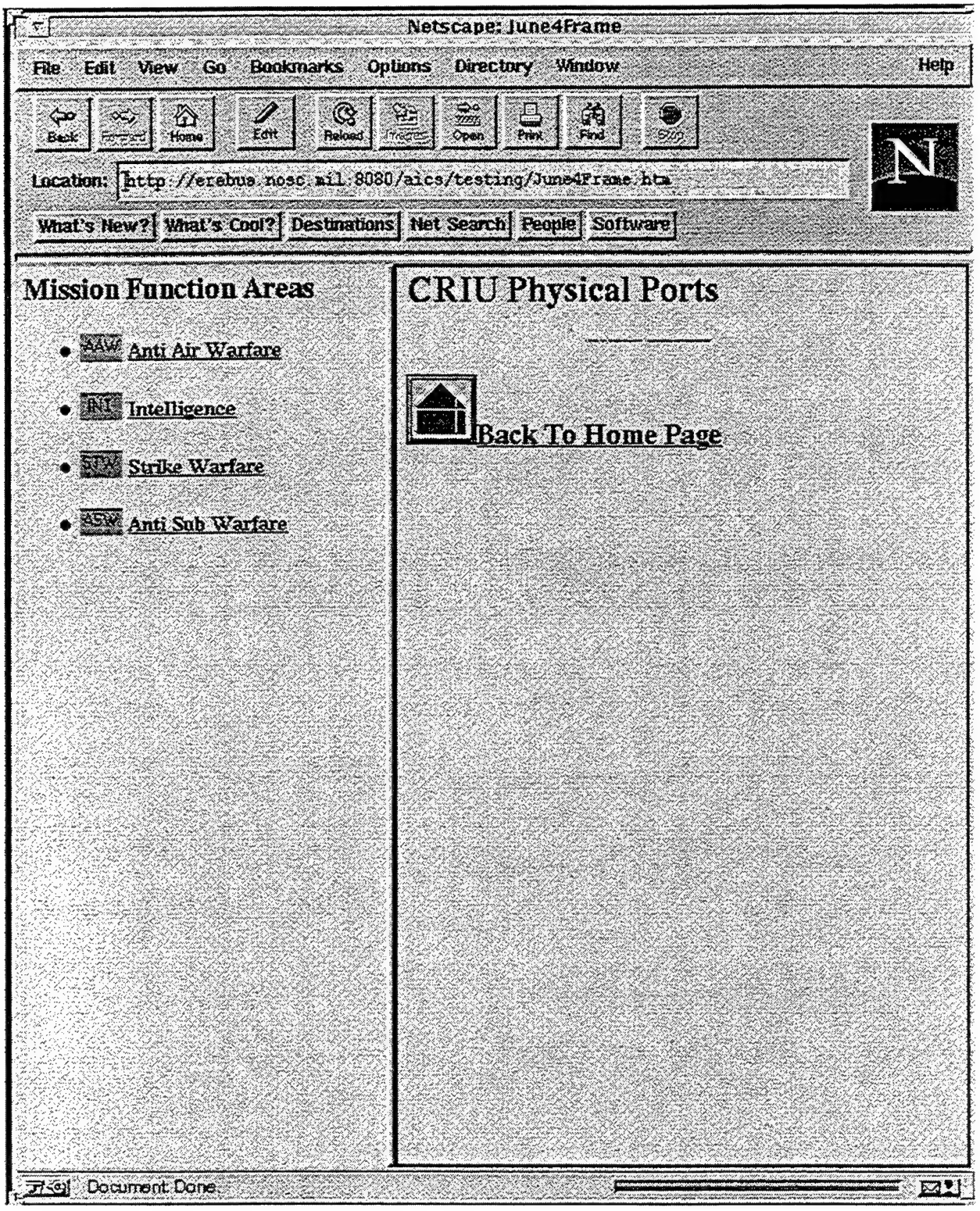

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
CRIU Physical Ports
Back To Home Page
Document Done.

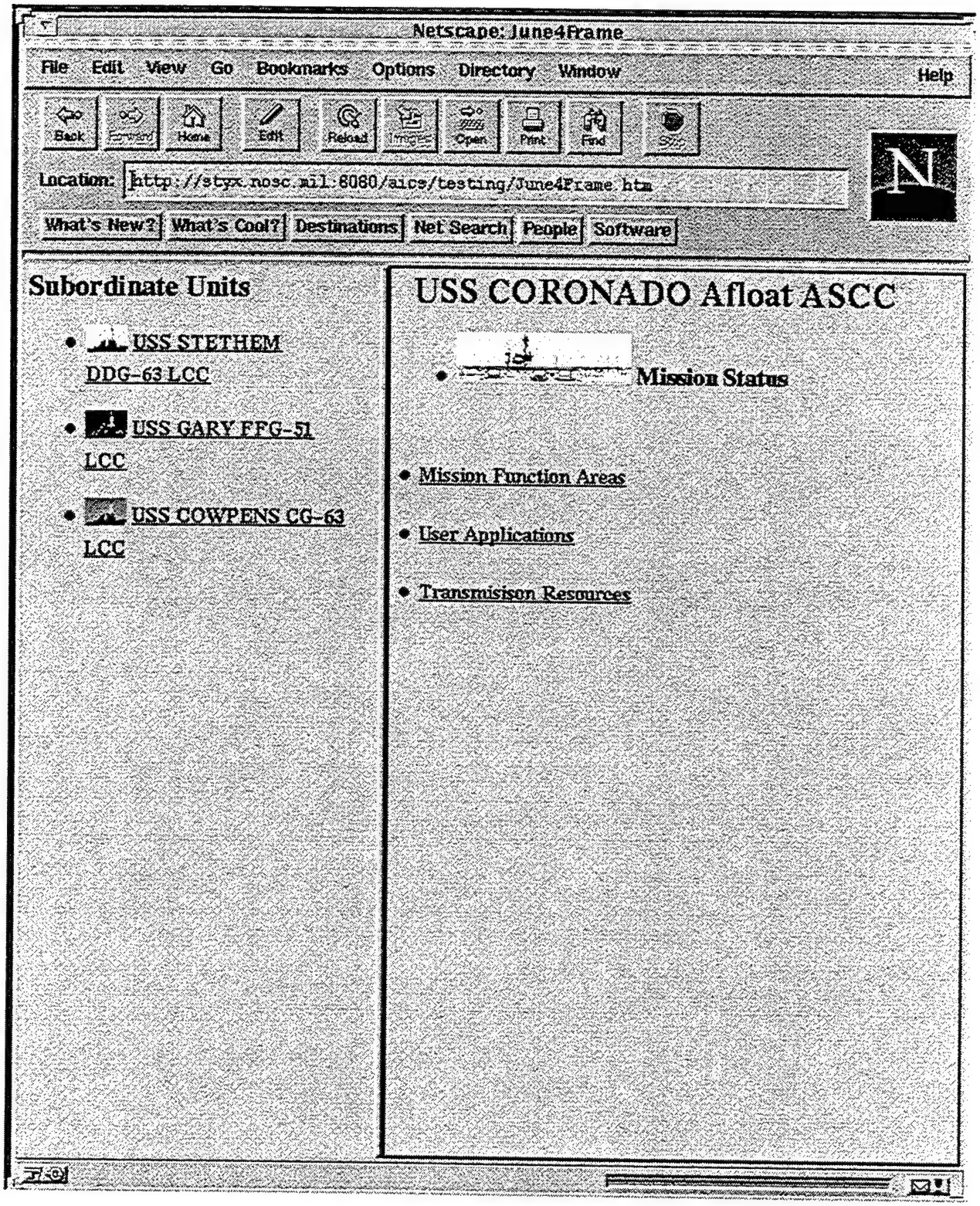

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
UHF CAP Physical Ports
Back To Home Page

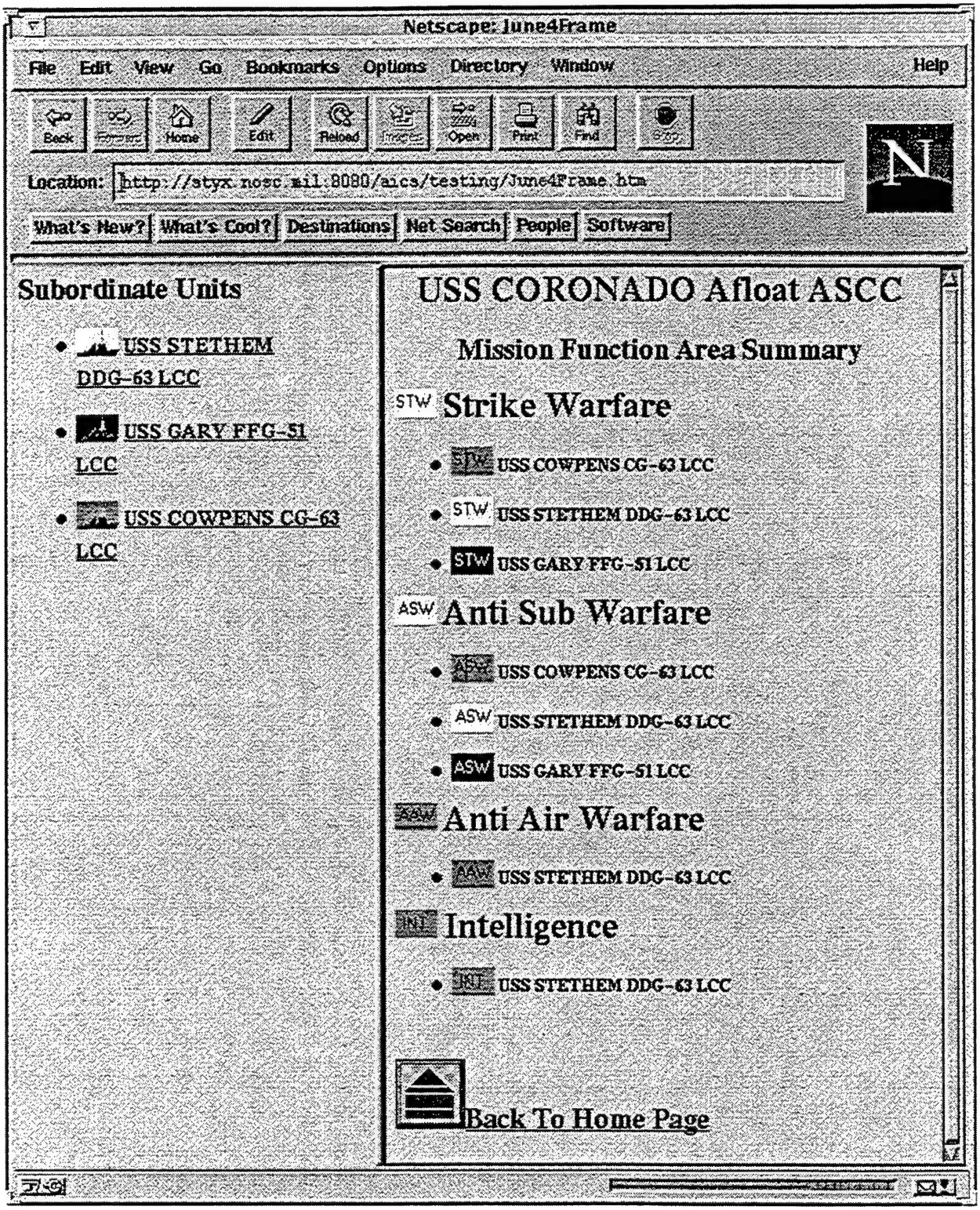

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
Anti Air Warfare
Intelligence
Strike Warfare
Anti Sub Warfare
Topscene Transmission Resources
USS STETHEM - Challenge Athena
Back To Home Page

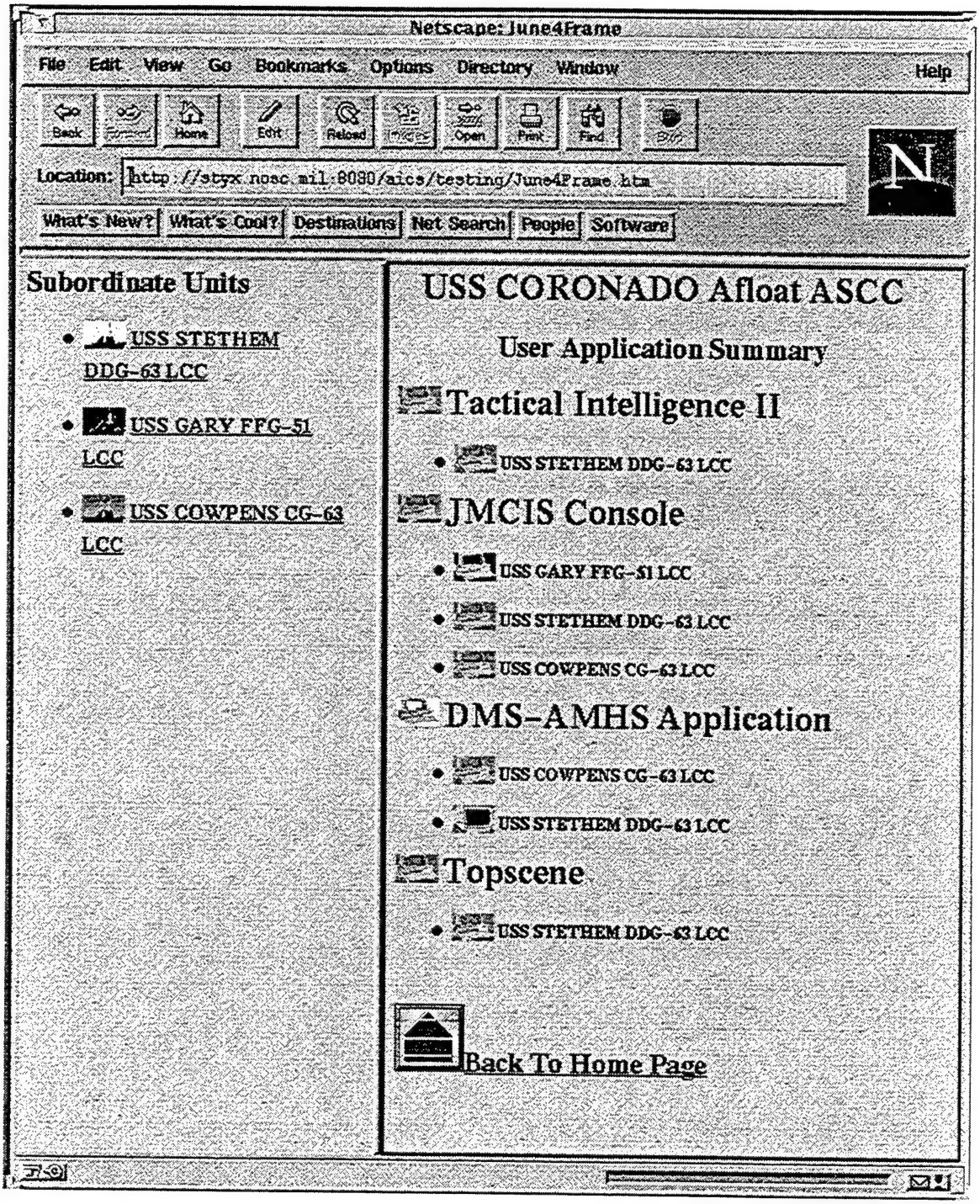

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
USS STETHEM – Challenge Athena Equipment
Challenge Athena CAP
CRIU
Back To Home Page
Launch mail window, and check for new mail

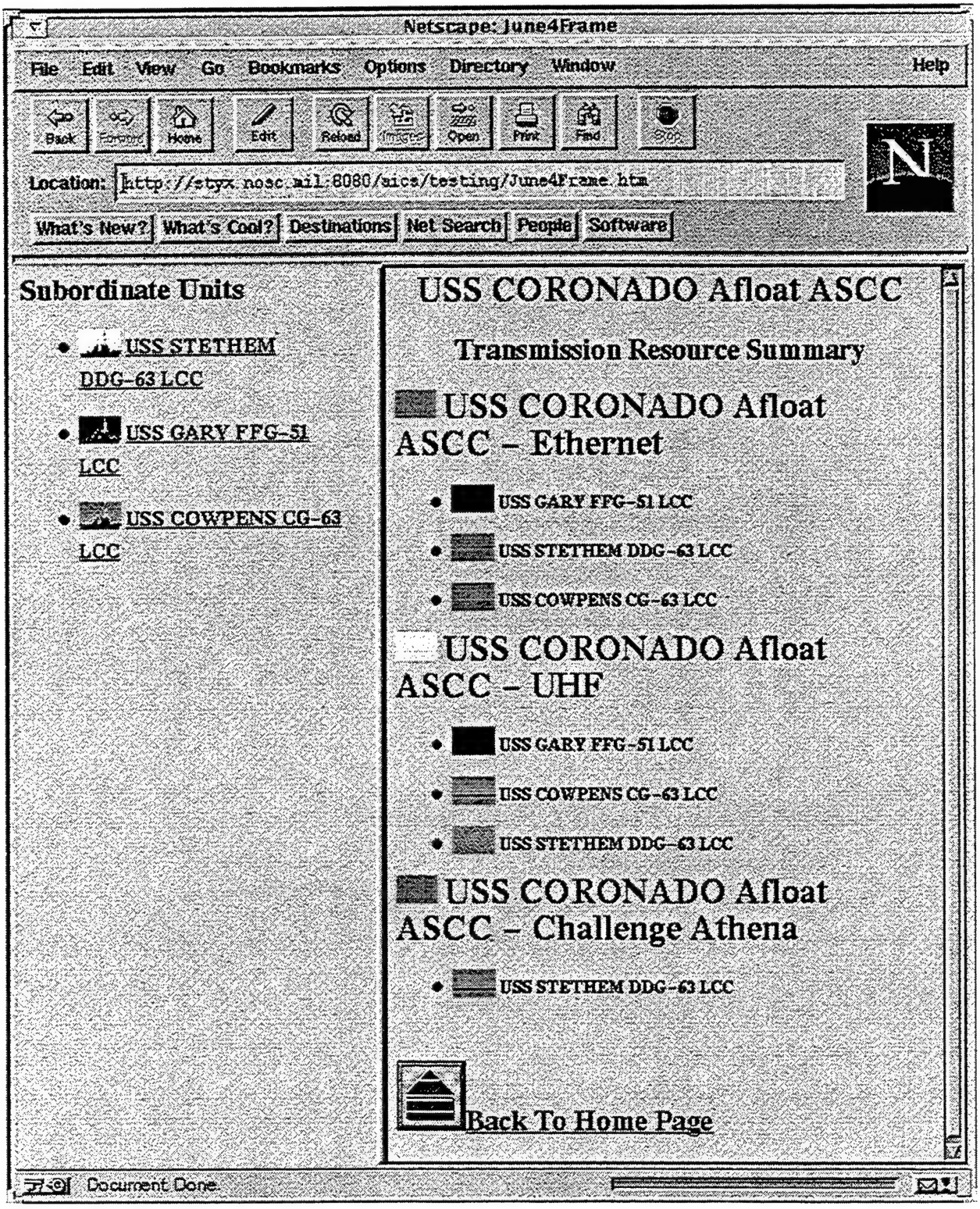

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
Challenge Athena CAP Physical Ports
Back To Home Page

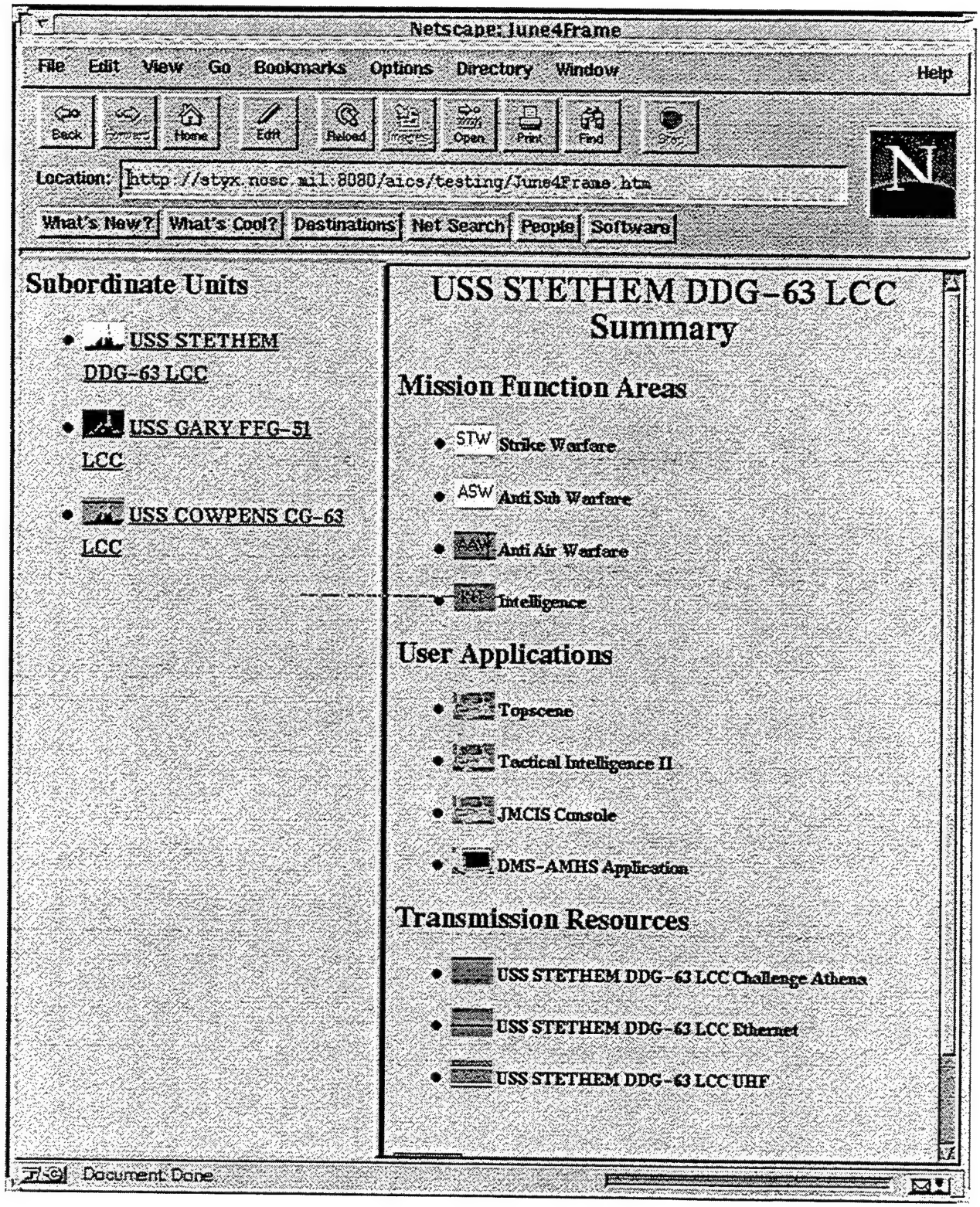

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://erebus.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Mission Function Areas
AAW Anti Air Warfare
INT Intelligence
STW Strike Warfare
ASW Anti Sub Warfare
CRIU Physical Ports
Back To Home Page
Document Done

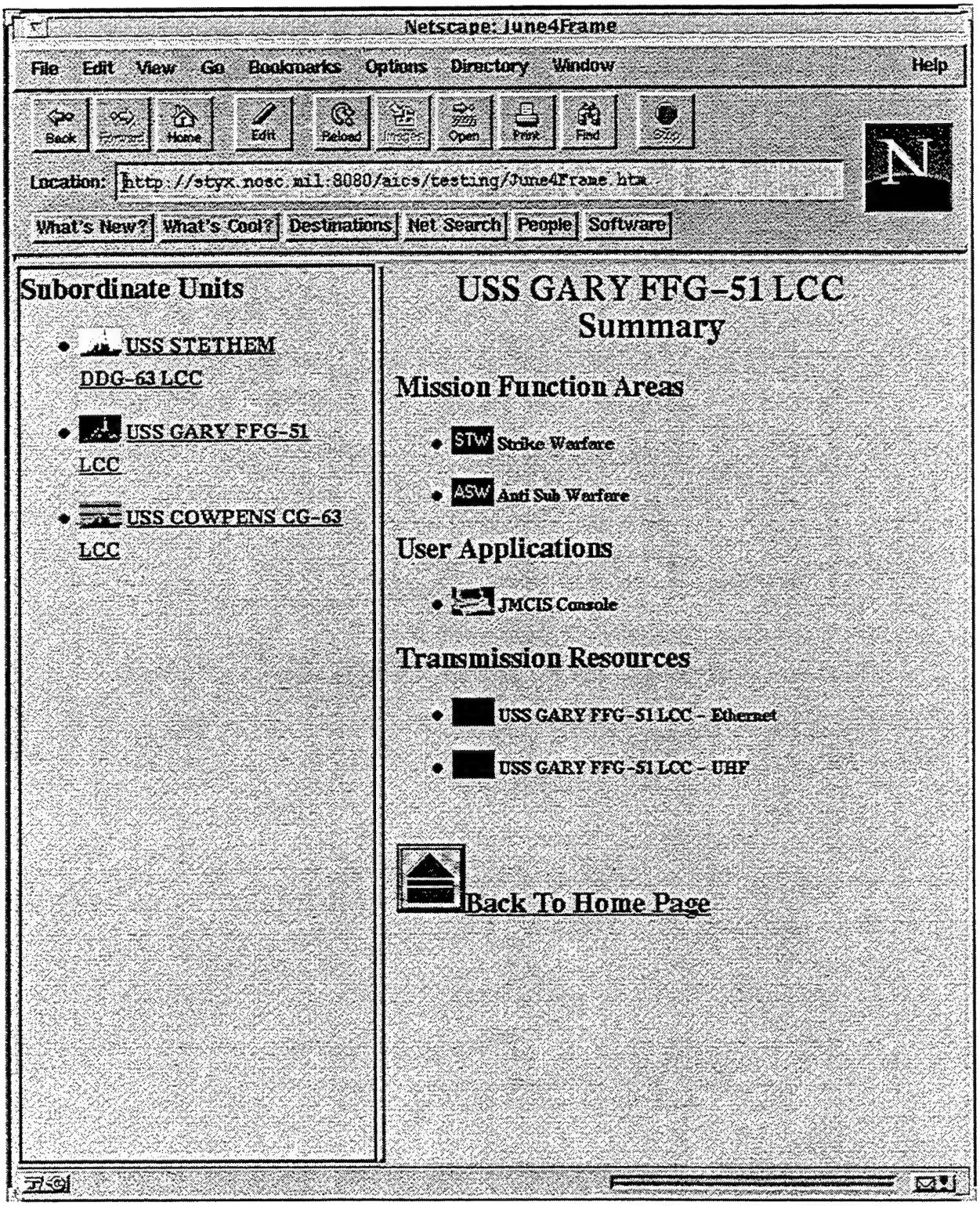

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS CORONADO Afloat ASCC
Mission Status
Mission Function Areas
User Applications
Transmisison Resources

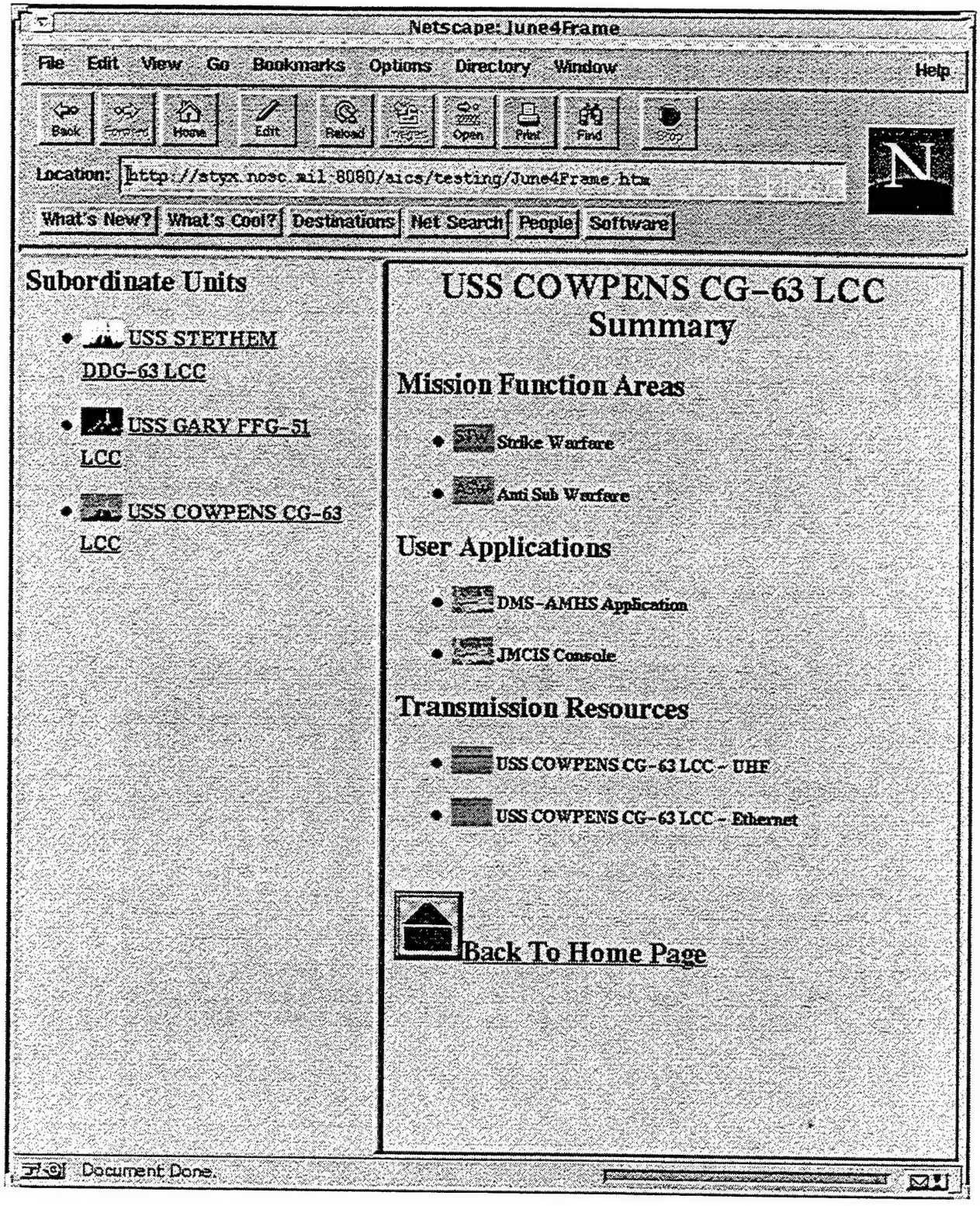

Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS CORONADO Afloat ASCC
Mission Function Area Summary
STW Strike Warfare
USS COWPENS CG-63 LCC
STW USS STETHEM DDG-63 LCC
STW USS GARY FFG-51 LCC
ASW Anti Sub Warfare
ASW USS COWPENS CG-63 LCC
ASW USS STETHEM DDG-63 LCC
ASW USS GARY FFG-51 LCC
AAW Anti Air Warfare
AAW USS STETHEM DDG-63 LCC
INT Intelligence
INT USS STETHEM DDG-63 LCC
Back To Home Page


Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS CORONADO Afloat ASCC
User Application Summary
Tactical Intelligence II
USS STETHEM DDG-63 LCC
JMCIS Console
USS GARY FFG-51 LCC
USS STETHEM DDG-63 LCC
USS COWPENS CG-63 LCC
DMS-AMHS Application
USS COWPENS CG-63 LCC
USS STETHEM DDG-63 LCC
Topscene
USS STETHEM DDG-63 LCC
Back To Home Page


Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/uics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS CORONADO Afloat ASCC
Transmission Resource Summary
USS CORONADO Afloat ASCC – Ethernet
USS GARY FFG-51 LCC
USS STETHEM DDG-63 LCC
USS COWPENS CG-63 LCC
USS CORONADO Afloat ASCC – UHF
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS STETHEM DDG-63 LCC
USS CORONADO Afloat ASCC – Challenge Athena
USS STETHEM DDG-63 LCC
Back To Home Page
Document Done


Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS STETHEM DDG-63 LCC Summary
Mission Function Areas
STW Strike Warfare
ASW Anti Sub Warfare
AAW Anti Air Warfare
Intelligence
User Applications
Topscene
Tactical Intelligence II
JMCIS Console
DMS-AMHS Application
Transmission Resources
USS STETHEM DDG-63 LCC Challenge Athena
USS STETHEM DDG-63 LCC Ethernet
USS STETHEM DDG-63 LCC UHF
Document Done


Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS GARY FFG-51 LCC Summary
Mission Function Areas
STW Strike Warfare
ASW Anti Sub Warfare
User Applications
JMCIS Console
Transmission Resources
USS GARY FFG-51 LCC - Ethernet
USS GARY FFG-51 LCC - UHF
Back To Home Page


Netscape: June4Frame
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://styx.nosc.mil:8080/aics/testing/June4Frame.htm
What's New? What's Cool? Destinations Net Search People Software
Subordinate Units
USS STETHEM DDG-63 LCC
USS GARY FFG-51 LCC
USS COWPENS CG-63 LCC
USS COWPENS CG-63 LCC Summary
Mission Function Areas
Strike Warfare
Anti Sub Warfare
User Applications
DMS-AMHS Application
JMCIS Console
Transmission Resources
USS COWPENS CG-63 LCC - UHF
USS COWPENS CG-63 LCC - Ethernet
Back To Home Page
Document Done.

LIST OF REFERENCES

Casey R., Naval Command Control and Ocean Surveillance Center (NRaD Code 8205), *ADNS Implementation Working Paper*, NRaD, July 15, 1997.

Concentric Network Corporation, http://www.concentric.net/~tkvallil/snmp.html

Deri L., IBM Zurich Research Lab, "IBM-HTTP-based SNMP and CMIP Network Management" – Internet draft, ftp://ietft.org/internet-drafts/draft-deri-http-mgmt-00.txt

Hewlett Packard white paper, "Riding the Internet Wave, Ensuring Safe, Solid Internet Services for the Enterprise" – Internet draft, http://www.hp.com

Jacobs E., Inchiosa, M., Guman, L., and Barber C., *Automated integrated Communications Systems (AICS) Integrated Network Manager Prototype Documentation, Technical Report 1735*, NRaD, January, 1997.

Leinwand A. and Fang K., *Network Management, A Practical Perspective*, second edition, Addison-Wesley Publishing Co., 1996.

Naval Command Control and Ocean Surveillance Center (NRaD Code 80), *Automated Integrated Communication System (AIC) Network Management Architecture for the Advanced Digital Network System (ADNS)*, NRaD, September 30, 1996.

Space and Naval Warfare Systems Command, PMW 176, *Joint Maritime Communications System (JMCOMS) Integrated Network Management (INM) Technical Approach*, draft revision 2, April 21, 1997.

Sridhar, S., *Managing Enerprise Networks Using the World Wide Web*, Code SM/SR Department of Systems Management, Naval Postgraduate School (NPS), January 15, 1997.

Stallings, W., *SNMP, SNMPv2, and CMIP, The Practical Guide to Network-Management Standards*, Addison-Wesley Publishing Co., 1993.

Stallings, W., *Data and Computer Communications*, fourth edition, Prentice Hall, 1994.

Stevenson, D., *Network Management, What it is and what it isn't*, http://netman.cit.buffalo.edu.Doc/DStevenson/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Mr. Bill Jacobs 1
   NCCOSC RDTE Div
   53560 Hull Street
   San Diego, CA 92152-5001

4. Mr. Lewis Gutman 1
   NCCOSC RDTE Div
   53560 Hull Street
   San Diego, CA 92152-5001

5. Mr. Roger Casey 1
   NCCOSC RDTE Div
   53560 Hull Street
   San Diego, CA 92152-5001

6. Mr. Mark Evans 1
   NCCOSC
   53560 Hull Street
   San Diego, CA 92152-5001

7. Mr. Marlan Kvigne 1
   NCCOSC
   53560 Hull Street
   San Diego, CA 92152-5001

8. CAPT Joseph Delpino, USN 1
   GBS Joint Program Office
   Skyline 5/Room 9095
   5111 Leesburg Pike
   Falls Church, VA 22041-3205

9. CAPT Richard Mead 1
   COMMANDANT (6-0)
   U.S. Coast Guard
   Washington, DC 20593

10. Prof. Mike Sovereign 1
Code C3
Naval Postgraduate School
Monterey, CA 93943

11. Prof. Rex Buddenberg 1
Code SM/Bu
Naval Postgraduate School
Monterey, CA 93943

12. LT Eric Andalis 2
6929 Beagle St
San Diego, CA 92111